Version 1.6, Oktober 2010



Xerox Secure Access Unified ID System®

Systemhandbuch

Übersetzung:
Xerox
CTC European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
Großbritannien

Inhalt

Sicherheitshinweise 1

Diese Sicherheitshinweise genau lesen und beachten, damit das Gerät sicher und den gesetzlichen Bestimmungen entsprechend betrieben wird.

Das Gerät wurde speziell entwickelt und getestet, um strenge Sicherheitsbestimmungen zu erfüllen. Hierbei handelt es sich unter anderem um die sicherheitstechnische Zulassung und die Einhaltung geltender Umweltstandards.

Vor der Inbetriebnahme des Geräts die nachstehenden Anweisungen sorgfältig lesen und bei Bedarf darauf zurückgreifen, um einen sicheren Betrieb des Geräts zu gewährleisten.


ACHTUNG: Jede unbefugte Veränderung, einschließlich der Erweiterung des Leistungsumfangs durch neue Funktionen und den Anschluss externer Geräte, kann zum Verlust der Produktzertifizierung führen. Detaillierte Informationen hierzu können beim Xerox-Partner erfragt werden

Netzanschluss

Das im Lieferumfang des Geräts enthaltende Netzteil ist an eine Steckdose anzuschließen, die die Anforderungen auf dem Typenschild erfüllt. Im Zweifelsfall den lokalen Stromversorger um Rat fragen.

Sicherheit des elektrischen Betriebs

- Nur das im Lieferumfang des Geräts enthaltene Netzteil verwenden.
- Den Installationsort so wählen, dass das Netzkabel außerhalb der Gehbereiche verlegt werden und niemand auf das Kabel oder das Netzteil treten kann.
- Keine Gegenstände auf das Netzkabel stellen.
- Unter den nachfolgenden Bedingungen ist unverzüglich das Gerät auszuschalten und der Netzstecker des Geräts zu ziehen. Dann einen autorisierten Servicetechniker rufen, um das Problem zu beheben.
    - Entwicklung ungewöhnlichen Geruchs
    - Netzkabel beschädigt
    - Sicherung durchgebrannt, Sicherungsautomat oder anderer Schutzschalter hat angesprochen
    - Gerät wurde Wasser ausgesetzt
    - Teil des Geräts beschädigt

Trennung vom Stromnetz

Zur Trennung des Geräts vom Stromnetz das Netzkabel abziehen. Um die Stromversorgung des Geräts ganz zu unterbrechen, den Netzstecker ziehen.

Rechtliche Informationen

Hochfrequenzenergie

United States, Canada

Hinweis: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used with this equipment to maintain compliance with FCC regulations in the United States

Canada

This Class "B" digital apparatus complies with Canadian ICES-003.

Cet appareil Numérique de la classe "B" est conforme à la norme NMB-003 du Canada.

Europa



Durch Kennzeichnung dieses Produkts mit dem CE-Zeichen erklärt sich Xerox bereit, den folgenden Richtlinien der Europäischen Union zu entsprechen (mit Wirkung vom siehe Datum):

12. Dezember 2006:	Richtlinie 2006/95/EG des Europäischen Parlaments und des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen.
15. Dezember 2004:	Richtlinie 2004/108/EG des Europäischen Parlaments und des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit und zur Aufhebung der Richtlinie 89/336/EWG.
9. März 1999:	Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität.

Der vollständige Text der Konformitätserklärung einschließlich der Definition der entsprechenden Richtlinien sowie der jeweiligen Standards ist über den Xerox-Partner erhältlich.



- Um eine fehlerfreie Funktion dieses Geräts in der Nähe von ISM-Geräten (Hochfrequenzgeräte für industrielle, wissenschaftliche, medizinische und ähnliche Zwecke) zu gewährleisten, ist es erforderlich, dass die Störstrahlung dieser Geräte reduziert oder auf andere Weise begrenzt wird.
- Gemäß der EU-Richtlinie 89/336/EWG müssen für dieses Gerät abgeschirmte Schnittstellenkabel verwendet werden.

Richtlinien für RFID-Geräte

Das mit diesem Produkt gelieferte Lesegerät erzeugt mit einer Induktionsschleife als RFID (Radio Frequency Identification) 13,56 MHz. Dieses RFID-Gerät entspricht den in der Richtlinie 1999/5/EG des Europäischen Rates sowie in sämtlichen nationalen gesetzlichen Regelungen enthaltenen Vorgaben.

Der Betrieb des Geräts unterliegt zwei Bedingungen: 1.) Das Gerät darf keine schädliche Interferenz erzeugen und 2.) das Gerät muss jegliche empfangenen Interferenzen, einschließlich solcher, durch die unerwünschte Betriebsbedingungen verursacht werden, akzeptieren.

Durch Änderungen an dem Gerät, die nicht ausdrückliche von Xerox genehmigt wurden, kann das Rechts auf den Betrieb des Geräts für den Nutzer hinfällig werden.

Recycling und Entsorgung des Geräts

Bei der Entsorgung des Geräts ist zu beachten, dass es Blei, Quecksilber und andere Stoffe enthalten kann, deren Entsorgung bestimmten Umweltschutzbestimmungen unterliegt. Der Gehalt an Blei und Quecksilber entspricht bei Markteinführung des Geräts den einschlägigen internationalen Bestimmungen.

Europäische Union

Entsorgungsinformationen für gewerbliche Nutzer



Dieses Symbol auf dem Gerät bedeutet, dass das Gerät in Übereinstimmung mit örtlichen Vorschriften entsorgt werden muss.

Elektrische und elektronische Altgeräte müssen gemäß europäischen Vorschriften entsorgt werden.

Vor der Entsorgung von Geräten beim örtlichen Xerox-Partner erkundigen, ob das Gerät eventuell zurückgenommen wird.

North America (USA, Canada)

Xerox operates a worldwide equipment take back and reuse/recycle program. Contact your Xerox sales representative (1-800-ASK-XEROX) to determine whether this Xerox product is part of the program. For more information about Xerox environmental programs, visit http://www.xerox.com/environment

If you are managing the disposal of your Xerox product, please note that the product may contain lead, mercury, Perchlorate, and other materials whose disposal may be regulated due to environmental considerations. The presence of these materials is fully consistent with global regulations applicable at the time that the product was placed on the market. For recycling and disposal information, contact your local authorities. In the United States, you may also refer to the Electronic Industries Alliance web site: http://www.eiae.org

Perchlorate Material – This product may contain one or more Perchlorate-containing devices, such as batteries. Special handling may apply; please see http://www.dtsc.ca.gov/hazardouswaste/perchlorate

Entsorgungsinformationen für private Nutzer



Mit diesem Symbol versehene Geräte dürfen nicht dem normalen Abfallprozess zugeführt werden.

Geräte mit diesem Symbol sind gemäß europäischer Richtlinien zur Entsorgung von elektrischen und elektronischen Geräten vom normalen Hausmüll zu trennen.

Privathaushalte innerhalb eines EU-Mitgliedstaates sind berechtigt, gebrauchte elektrische und elektronische Geräte gebührenfrei bei den entsprechenden Sammelstellen abzugeben. Weitere Auskünfte erteilen die örtlichen Behörden.

In einigen Mitgliedsstaaten sind die Einzelhändler verpflichtet, beim Neukauf alte Geräte kostenlos zurückzunehmen. Weitere Auskünfte erteilen die Einzelhändler.

Andere Länder

Auskünfte beim örtlichen Abfallentsorgungsträger einholen.

Kontaktdaten für Informationen zu Umwelt- und Arbeitssicherheit

Kontaktdaten

Weitere Informationen zur Umwelt- und Arbeitssicherheit sind unter folgender Rufnummer bzw. Internetadresse erhältlich:

USA: 1-800 828-6571

Kanada: 1-800 828-6571

Europa: +44 1707 353 434

http://www.xerox.com/environment safety information US (Informationen zur Produktsicherheit für die USA)

http://www.xerox.com/environment_europe (Informationen zur Produktsicherheit für Europa)

Checkliste zur Installation

2

Das Installationshandbuch und das Systemhandbuch zu Xerox Secure Access enthalten schrittweise Anleitungen zur Installation und Konfiguration des Secure Access-Servers und der MFG. In der nachfolgenden Tabelle ist die Reihenfolge der Arbeitsschritte angegeben, die je nach Secure Access-Hardwarekonfiguration auszuführen sind.

Schritte (*) = obligatorisch	Xerox Secure Access mit USB-Kartenleser	Xerox Secure Access mit Authentifizierungsgerät und Kartenleser
Installationshandbuch		
1. Kapitel 3, „Installationsübersicht", lesen	*	*
2. Kapitel 4, „Installation des Secure Access-Servers", Abschnitt 1: „Vorbereitung von Netzwerk und Datenbank"	*	*
3. Kapitel 4, „Installation des Secure Access-Servers", Abschnitt 2: „Ausführung des Installationsassistenten"	*	*
4. Kapitel 5, „Einrichtung der Secure Access-Hardware", Schritt 1: „Einstellung der IP-Adresse des Authentifizierungsgeräts"	Überspringen	*
5. Kapitel 5, „Einrichtung der Secure Access-Hardware", Schritt 2: „Installation des Secure Access-Authentifizierungsgeräts"	Überspringen	*
6. Kapitel 5, „Einrichtung der Secure Access-Hardware", Schritt 3: „Anschluss der Hardware"	Überspringen	*
7. Kapitel 5, „Einrichtung der Secure Access-Hardware", Schritt 4: „Installation des Secure Access-USB-Kartenlesers"	*	Überspringen
Systemhandbuch		
8. Kapitel 3, „Überblick über Secure Access", lesen	*	*
9. Kapitel 4: „Konfigurationsverfahren", Schritt 1: „Konfigurierung des MFGs für die Netzwerkauthentifizierung über Secure Access"	*	*
10. Kapitel 4: „Aufnahme von MFG in die Secure Access-Datenbank"	*	*

Schritte (*) = obligatorisch	Xerox Secure Access mit USB-Kartenleser	Xerox Secure Access mit Authentifizie-rungsgerät und Kartenleser
11. Kapitel 4: „Zuordnung eines Secure Access-Authentifizierungsgeräts zu einem MFG“	Überspringen	*
12. Kapitel 4: „Konfiguration des Follow-You-Drucks“ (optional)	*	*
13. Kapitel 4: „Einrichtung der Authentifizierungsparameter“	*	*
14. Kapitel 4: „Import und Synchronisierung von Benutzerkonten“	*	*
15. Kapitel 4: „Konfiguration des Diensts ‚Release My Documents‘“	*	*

3 Überblick über Secure Access

Themen dieses Kapitels:

Nachdem der Xerox Secure Access Unified ID System®-Server installiert und die Authentifizierungsgeräte bzw. das Secure Access-USB-Kartenlesegerät eingerichtet wurden, mithilfe dieses Handbuchs der Secure Access-Datenbank Multifunktionsgeräte (MFG) hinzufügen und so die Kommunikation zwischen dem Server und den Authentifizierungsgeräten ermöglichen. Anhand dieses Handbuchs können komplexe Konfigurationsaufgaben für alle Komponenten und Funktionen von Secure Access durchgeführt werden.

Dieses Kapitel enthält Informationen über:

- Hardware- und Softwarekomponenten von Xerox Secure Access
- Zugriff auf Secure Access Manager zur Verwaltung des Systems

Informationen über Secure Access

Secure Access Unified ID System® ist ein System, das den Zugriff auf die Druck-, Fax-, Kopier- und Scan-Funktionen von Xerox-Multifunktionsgeräten (MFG) kontrolliert. Wenn ein Benutzer auf ein durch Secure Access kontrolliertes Gerät zugreifen möchte, muss er seine Karte entweder durch ein Kartenlesegerät ziehen oder an einem Transponderkartenlesegerät vorzeigen. Das Steuerpult vorn am MFG wird nur aktiviert, wenn die Kontodaten des Benutzers durch den Secure Access-Server authentifiziert wurden.

Unter Verwendung eines systemeigenen Protokolls (Convenience Authentication Protocol) kontaktiert das Secure Access-Authentifizierungsgerät den Secure Access-Server über eine Ethernet-Netzwerkverbindung, um die von der Magnetstreifen- oder Transponderkarte gelesenen Informationen zu prüfen. Bei Einsatz eines USB-Kartenlesegeräts erfolgt die Kommunikation zwischen Gerät und Secure Access-Server direkt. Enthält die Karte gültige Benutzerangaben, wird das Steuerpult entsperrt und ist einsatzbereit. Wenn der Benutzer nicht verifiziert werden konnte, bleibt die Sperre des MFGs bestehen, so dass der Benutzer das Gerät nicht nutzen kann.

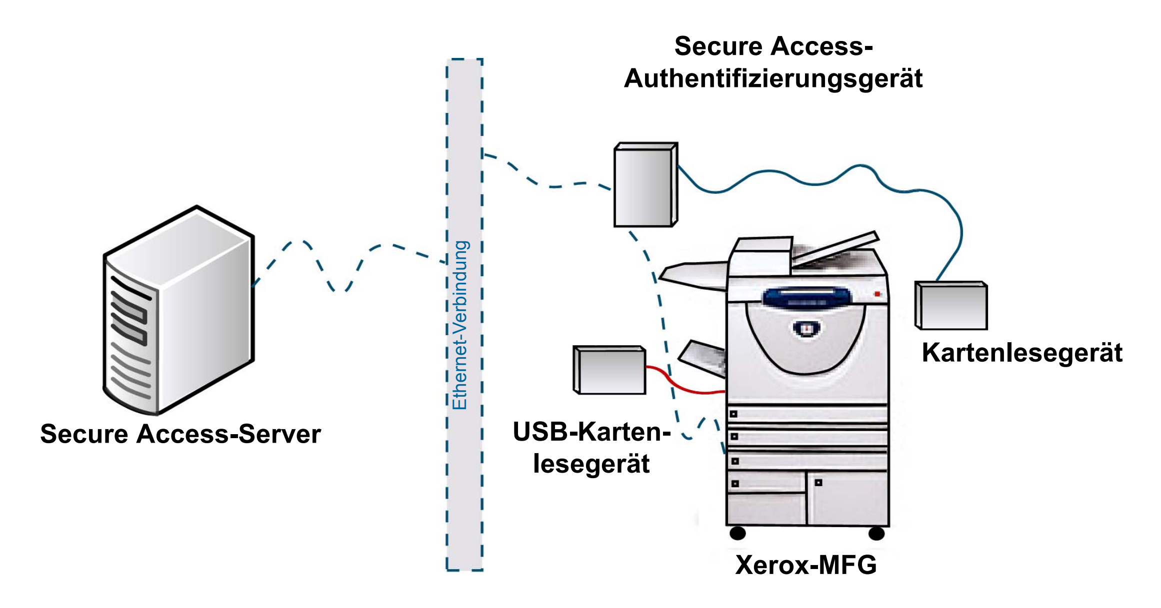


Abbildung 3-1: Komponenten der Secure Access-Lösung

Wenn der Benutzer Dokumente scannen möchte, stellt der Secure Access-Server dem entsprechenden MFG die Netzwerkbenutzerkennung bereit. Auf dem MFG wird dann anhand der Kennung die Single Sign-On-Funktionalität implementiert und eine automatische Authentifizierung für den Scanbetrieb durchgeführt.

Secure Access-Komponenten

Die Lösung umfasst zwei Hauptkomponenten:

1. **Secure Access-Authentifizierungsgerät**, das aus einem Authentifizierungsterminal und einem externen Kartenlesegerät besteht. Benutzer greifen nicht auf das Authentifizierungsterminal zu.

   Das Kartenlesegerät ist über ein serielles Kabel nur an das Authentifizierungsgerät angeschlossen. Es besteht keine direkte Verbindung zum MFG. Weitere Informationen zur Einrichtung und Montage sind dem *Installationshandbuch* zu entnehmen.

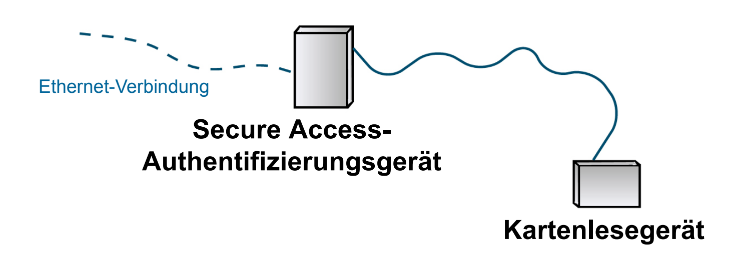


Abbildung 3-2: Komponenten des Secure Access-Authentifizierungsgeräts

-Oder-

1. **Secure Access-Server-USB-Kartenlesegerät**, das an das MFG angeschlossen ist. Weitere Informationen zur Einrichtung und Montage sind dem Installationshandbuch zu entnehmen.
2. **Secure Access-Server**, der sich aus folgenden Komponenten zusammensetzt:
   - Core Authentication Server (CAS)
   - Device Control Engine (DCE)
   - Document Routing Engine (DRE)
   - Secure Access Manager (Verwaltungsprogramm)

   Hinweis: Diese Komponenten können auf einem einzelnen Server installiert oder auf mehrere Server verteilt werden. Im manchen Implementierungen sind mehrere DCEs oder DREs erforderlich. Ausführliche Informationen sind dem *Installationshandbuch* zu entnehmen.

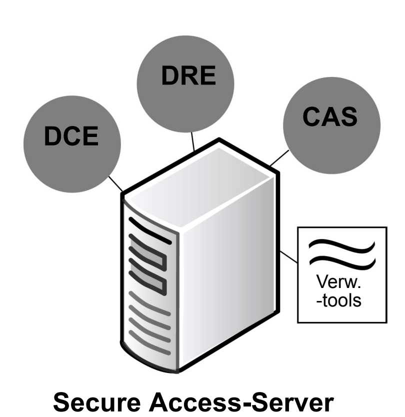


Abbildung 3-3: Secure Access-Serverkomponenten

Die Komponenten des Servers kommunizieren über designierte Ports. Jede Komponente „horcht" einen bestimmten Port auf Informationen oder Anforderungen von den anderen Komponenten ab. Eine komplette Liste mit den Portzuordnungen der einzelnen Komponenten befindet sich im Abschnitt Portzuweisungen Seite 45.

Core Authentication Server (CAS)

Auf dem Core Authentication Server (CAS) residiert die Datenbank, die alle Benutzer- und MFG-Daten enthält.

Für jede Secure Access-Installation ist eine vorinstallierte Datenbank erforderlich. Der CAS nutzt die Datenbankinstanz zur Erstellung einer Kontendatenbank, die sämtliche Benutzer- und Gerätedaten enthält. Informationen zu den unterstützten Datenbanken sind im *Installationshandbuch* unter „Systemanforderungen des Secure Access-Servers" enthalten.

Device Control Engine (DCE)

Die DCE (Device Control Engine) wickelt die gesamte Kommunikation mit den MFG ab. Wenn ein Benutzer die Kopier-, Scan- oder Faxfunktionalität eines MFG nutzen möchte, muss zunächst das Kartenlesegerät bedient werden. Eine Magnetstreifen- oder Transponderkarte löst eine Zugriffsanforderung aus.

Das Authentifizierungsgerät leitet die Anmeldeanforderung an die DCE weiter, welche dann den CAS auffordert, die Daten des zu der Karte gehörigen Benutzerkontos zu überprüfen. Dieser Prozess wird in den Abbildungen 4 und 5 dargestellt.

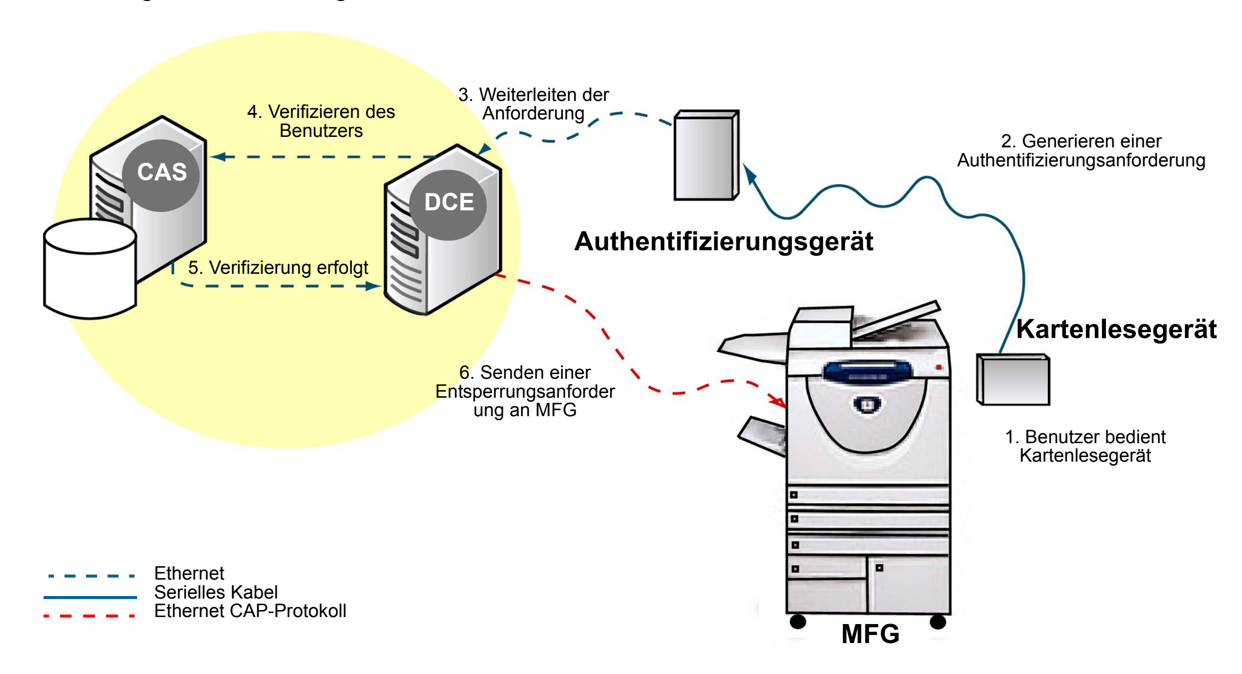


Abbildung 3-4: Benutzerauthentifizierung

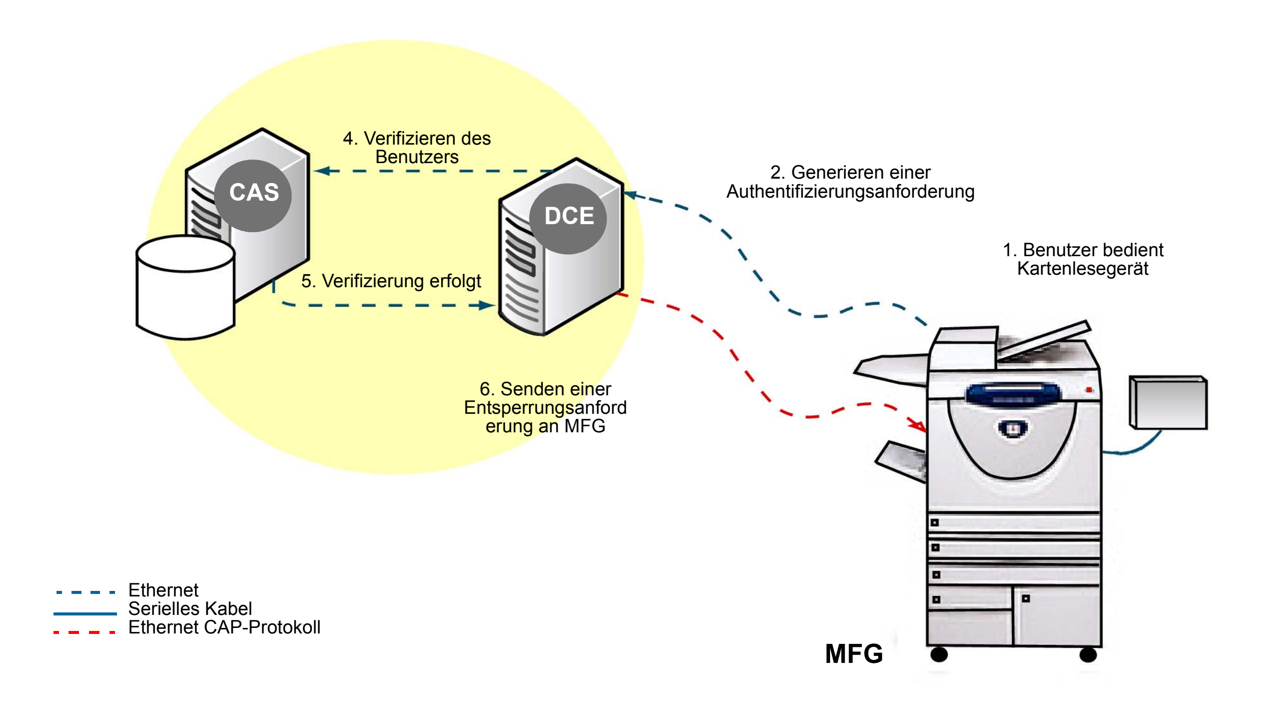


Abbildung 3-5: Benutzerauthentifizierung über USB-Kartenlesegerät

Document Routing Engine (DRE)

Bei der Document Routing Engine (DRE) handelt es sich um den Druckserver. Ihre Hauptfunktion liegt in der Leitung der Dokumente von den Arbeitsstationen der Benutzer zu den MFG. Eines typischer DRE-Workflow sieht wie folgt aus:

1. Ein Benutzer generiert eine Druckanforderung an ein MFG, das in der Secure Access Manager-Datenbank registriert ist.
2. Wenn der Benutzer über eine Druckerwarteschlange druckt, die einen Secure Access Manager-Port nutzt, hält die DRE den Druckauftrag auf dem Druckserver.
3. Meldet sich der Benutzer beim MFG an, durchsucht die DRE die für diesen Drucker (und/oder diese Gerätegruppe) in der Warteschlange befindlichen Aufträge und gibt jene frei, die von dem angemeldeten Benutzer übermittelt wurden.

   Hinweis: Ist der Dienst „Release My Documents“ installiert, kann der Benutzer die Warteschlange mit den geschützten Aufträgen einsehen und eigene Aufträge nach Bedarf freigegeben. Siehe Konfiguration des Diensts „Release My Documents“ Seite 40.

Wenn auf dem Gerät kein Secure Access-Port installiert ist, erfolgt der Druck des Auftrags ohne Überprüfung.

Wenn Druckaufträge in einer gesicherten Warteschlange gehalten werden sollen, kann der Follow-You-Druck konfiguriert werden. Um diese Funktion zu aktivieren, muss für das MFG anstelle eines Standardports die Nutzung eines Secure Access-Ports konfiguriert werden. Der Portmonitor lässt sich in das Windows-Drucksubsystem integrieren und agiert als Teil des Spooler-Diensts. So kann der Portmonitor Druckaufträge empfangen und in einer gesicherten virtuellen Warteschlange halten, bis ein verifizierter Benutzer sie zur Verarbeitung auf einem bestimmten MFG freigibt.

Wenn der Follow-You-Druck aktiviert ist, muss sich der Benutzer zunächst beim MFG seiner Wahl authentifizieren (siehe Abbildung 3-4: Benutzerauthentifizierung ,Seite 16). Wenn die Authentifizierung erfolgreich ist, erhält der Benutzer Zugriff auf das Steuerpult des MFGs und kann, sofern der Dienst „Release My Documents“ installiert ist, die Druckerwarteschlange einsehen. Der Benutzer kann bestimmte oder alle Aufträge (falls konfiguriert) freigeben.

Änderungen an den Server-Komponenten

Änderungen, die in Secure Access Manager an der Konfiguration der Secure Access-Serverkomponenten (CAS, DRE, DCE) vorgenommen werden, wie beispielsweise das Hinzufügen neuer Secure Access-Geräte, werden erst nach mindestens 30 Sekunden wirksam.

Die Verzögerung bei der Aktualisierung von Server-Komponenten ist Bestandteil der CAS-Abruffunktion. Dies bedeutet, dass die Verzögerung länger sein kann, wenn der CAS während der Abrufperiode nach der Server-Aktualisierung aus irgendeinem Grund nicht verfügbar ist. Sobald die Verbindung wiederhergestellt ist, sendet der CAS die Änderungsdaten an die entsprechenden Komponenten.

Datenlesegeräte und Kartenverwendung

Die MFG-Funktionen sind gesperrt, bis ein Benutzer gültige Kontodaten zur Verfügung stellt. Dazu muss ein Benutzer seine Magnetstreifenkarte durch einen Magnetstreifenleser ziehen oder seine Transponderkarte am entsprechenden Lesegerät vorzeigen.

Wenn die Benutzerdaten durch den Core Authentication Server (CAS) authentifiziert wurden, wird das MFG entsperrt und ist einsatzbereit. Wenn der Benutzer seine Tätigkeiten abgeschlossen hat, kann er die Taste **Alles löschen** oder **Zugriff** auf dem MFG-Tastenfeld drücken, um sich abzumelden bzw. das Gerät zu sperren.

Secure Access ist mit externen Lesegeräten für Magnetstreifenkarten, HID-, EM Marin-, Hitag-, und Indala-Transponderkarten sowie Legic- und Mifar-Smartcards kompatibel. Alle Lesegeräte sind von Herstellerseite vorkonfiguriert und erfordern keine weitere Konfiguration.

Magnetstreifenlesegerät

Secure Access unterstützt externe Magnetstreifenlesegeräte. Benutzer können Überprüfungsdaten eingeben, indem sie eine codierte Magnetkarte durch das Kartenlesegerät ziehen. Das Magnetstreifenlesegerät liest fast alle Standard-Magnetkartenmedien auf Track 2 ein und akzeptiert standardmäßig oder benutzerdefiniert codierte Daten. Daten auf Track 1 stehen bei USB-Magnetstreifenlesegeräten zur Verfügung.

Verwendung eines Magnetstreifenlesegeräts

Instruktionen für Benutzer zur Eingabe von Daten über ein Magnetstreifenlesegerät:

1. Die Karte in die Führungsschiene einführen, wobei der Magnetstreifen weg vom Terminal weisen muss. Sicherstellen, dass die Karte fest gegen die Führung gedrückt wird.
2. Die Karte entlang der Führungsschiene ziehen und anschließend herausnehmen.

   Hinweis: Wenn die Karte schräg durchgezogen wird, nimmt das Terminal die Daten nicht an.

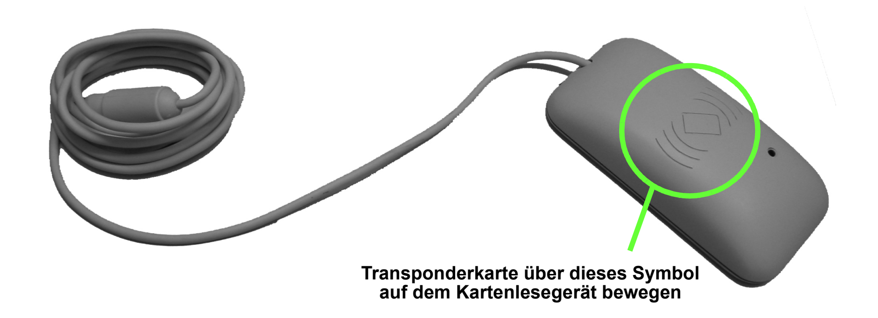
   Wenn das Terminal die Daten nicht lesen kann, leuchtet die LED-Anzeige rot auf. Die Karte erneut in die Führungsschiene einführen und durch das Lesegerät ziehen.

Kontaktlose Smartcards und Transponderkarten

Secure Access unterstützt kontaktlose Legic- und Mifare-Smartcards sowie EM-Marin, HID-, Hitag- und Indala-Transponderkarten. Benutzer können ihre Überprüfungsdaten eingeben, indem sie ihre Transponderkarte am externen Lesegerät vorzeigen und dabei einen Abstand von ca. 2,5 cm einhalten.

Verwenden einer Transponderkarte oder Smartcard

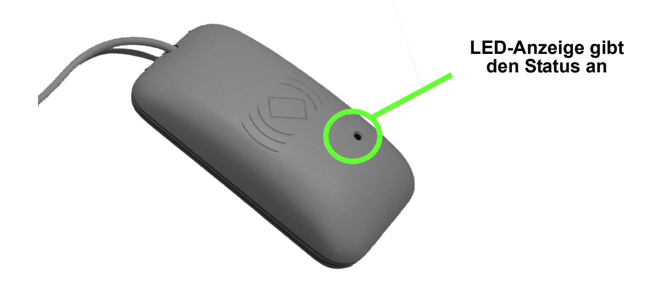
Um Daten mittels einer Transponderkarte oder Smartcard einzugeben, muss die Karte in einem Abstand von etwa 2,5 cm vom Transponderkartensymbol oben auf dem Kartenlesegerät vorgezeigt werden. Das Transponderkartenlesegerät auf dem Datenlesemodul ist an folgendem Symbol erkennbar:



Wenn der Vorgang ungültig ist, blinkt die LED-Anzeige rot.

Kartenlesesignale und -modi

Secure Access-Meldungen werden durch eine LED-Anzeige auf dem Kartenlesemodul angezeigt.



Die LED-Anzeige funktioniert bei beiden Lesegerättypen, sofern nicht anders angegeben, gleich. Folgende Signale können angezeigt werden:

LED-Signal	Bedeutung
Durchgehend rot	Das Authentifizierungssubsystem befindet sich im Leerlaufmodus; es signalisiert Einsatzbereitschaft, doch es ist keine aktive Sitzung vorhanden.
Durchgehend grün	Das Authentifizierungsgerät befindet sich im Bereitschaftsmodus, und es ist eine aktive Sitzung vorhanden. Dieser Zustand tritt auch bei Verwendung eines USB-Kartenlesegeräts ein, während das MFG gestartet wird und der Netzwerkcontroller noch nicht initialisiert wurde.

LED-Signal	Bedeutung
Langsames grünes Blinken	Daten vom Kartenlesegerät erhalten; es wird auf die Authentifizierung für die aktive Sitzung oder eine Benutzereingabe (z. B. in Form einer automatischen Kartenregistrierung oder einer Eingabe an der Eingabeaufforderung für die Freigabe aller Aufträge) gewartet.
Langsames rotes Blinken	Es besteht keine Verbindung zwischen Authentifizierungssubsystem und Server.
Schnelles rotes Blinken	Ungültige Karte, Zugang verweigert.

Das Authentifizierungssubsystem besitzt zwei Modi: Leerlauf- oder Bereitschaftsmodus.

Ein Authentifizierungssubsystem im Leerlaufmodus ist einsatzbereit. Wenn ein Benutzer eine Magnetstreifenkarte durchzieht, wechselt das Gerät in den Bereitschaftsmodus. Das Gerät kehrt in den Leerlaufmodus zurück, wenn ein Benutzer eine Transaktion beendet oder wenn es während eines auf dem MFG konfigurierbaren Zeitraums im Bereitschaftsmodus ungenutzt bleibt.

> Hinweis: Das Authentifizierungssubsystem wechselt bei der Aktivierung des Ruhezustands des MFGs zurück in den Leerlaufmodus.

Wenn sich das Gerät im Leerlaufmodus befindet, leuchtet die LED-Anzeige durchgehend rot.

Während des Bereitschaftsmodus leuchtet die LED-Anzeige auf dem Kartenlesegerät durchgehend grün, und der Benutzer kann das kontrollierte Gerät zur Durchführung einer Transaktion nutzen.

Verwaltung von Secure Access

Die gesamte Verwaltung erfolgt über das Tool Secure Access Manager. Secure Access Manager wird bei der Installation standardmäßig in das Startmenü eingefügt.

Zum Starten von Secure Access Manager Folgendes auswählen: **Start** > **Alle Programme** > **Xerox Secure Access** > **Secure Access Manager**.

> Hinweis: Für die Ausführung von Secure Access Manager auf dem Secure Access-Server sind Administratorrechte erforderlich.

Vor dem Öffnen des Tools Secure Access Manager muss der CAS, mit dem gearbeitet werden soll, ausgewählt werden. Die CAS-Überprüfung erfolgt über eine einzelne Authentifizierungsdatenbank. Daher muss der korrekte Datenbankname eingegeben oder über die bereitgestellte Liste ausgewählt werden.

Die Bedienungsoberfläche von Secure Access Manager ist in fünf Bereiche unterteilt. Wenn aus den verfügbaren Tools eine Funktion ausgewählt wird, wird der Inhalt des rechten Arbeitsbereichs aktualisiert, und es werden die verfügbaren Optionen angezeigt.

Einstellung der Sprache

Bei der Installation von Secure Access muss angegeben werden, welche Spracheinstellung für die Komponenten der Implementierung verwendet werden soll. Diese Einstellung gilt nur für die Bedienungsoberfläche von Secure Access Manager.

Die auf dem Steuerpult des MFGs angezeigte Sprache wird in den Geräteeinstellungen festgelegt. Der Secure Access-Server prüft die Spracheinstellung auf dem MFG jedes Mal, wenn ein Benutzer seine Karte durchzieht. Ist auf dem MFG eine andere Sprache als Deutsch, Englisch, Französisch, Italienisch oder Spanisch eingestellt, werden die Secure Access-Eingabeaufforderungen auf Englisch angezeigt.

Konfiguration und Verwaltung

4

Themen dieses Kapitels:

Der Begriff „Konfiguration“ bezieht sich auf die für die Kommunikation zwischen den MFG, den Authentifizierungsgeräten und dem Secure Access-Server erforderliche Softwarekonfiguration. Das auf Seite 24 beschriebene Verfahren befolgen, um optimale Ergebnisse zu erzielen.

Dieses Kapitel bietet Informationen zu folgenden Arbeitsgängen:

- Vollständige Erstkonfiguration
- Aufnahme von MFG in die Secure Access-Datenbank
- Zuordnung eines Secure Access-Authentifizierungsgeräts zu einem MFG, sofern kein USB-Kartenlesegerät verwendet wird
- Durchsetzung der Authentifizierung und Festlegung zusätzlicher Authentifizierungsoptionen
- Import und Synchronisierung von Benutzerkonten mit der Active Directory-Synchronisierung
- Überwachung von Authentifizierungsereignissen

Konfigurationsverfahren

Die Schritte in der nachstehenden Reihenfolge ausführen. Anderenfalls ist die Installation unvollständig.

Zunächst sicherstellen, dass der Secure Access-Server ordnungsgemäß installiert ist. Die Anleitungen im Installationshandbuch zu Xerox Secure Access Unified ID System® befolgen. Den CAS und mindestens eine DCE und DRE installieren.

1. **Konfigurierung des MFGs für die Netzwerkauthentifizierung über Secure Access**

   Dieser Arbeitsschritt erfolgt mithilfe der Internet-Services, auf die über einen Browser zugegriffen wird. Weitere Informationen zur Installation und Konfiguration von Xerox Secure Access auf dem Gerät befinden sich auf der System-CD des MFGs.

2. **Aufnahme von MFG in die Secure Access-Datenbank**

   Für jedes MFG einen Eintrag in Secure Access Manager erstellen. Jedes MFG einem bestimmten DRE-Druckserver zuordnen (falls erforderlich).

3. **Konfiguration des Follow-You-Drucks**

   Hinweis: Dieser Schritt ist nur dann erforderlich, wenn am Standort der Follow-You-Druck benötigt wird.

   Zur Konfiguration des Follow-You-Drucks Gerätegruppen erstellen, in denen Geräte mit gleichen Merkmalen gruppiert werden. Wenn der Benutzer ein Dokument an ein MFG innerhalb einer Gerätegruppe sendet, kann seine Authentifizierung an jedem MFG innerhalb der Gruppe erfolgen, und der auf diesem MFG zu druckende Auftrag kann aus der Warteschlange aufgerufen werden.

4. **Einrichtung der Authentifizierungsparameter**

   Die Parameter konfigurieren, die Secure Access für die Authentifizierung von Benutzerzugriffsanforderungen benötigt, einschließlich sekundärer Eingabeaufforderungen und Kartendateneinrichtung.

5. **Import und Synchronisierung von Benutzerkonten**

   Die Parameter für die Active Directory-Synchronisierung einrichten und anschließend vorhandene Benutzerkonten in die Secure Access-Datenbank importieren.

6. **Installation des Diensts „Release My Documents“**

   Mithilfe dieses Diensts können Benutzer am Steuerpult des MFGs geschützte Aufträge in der Druckwarteschlange anzeigen oder freigeben.

7. **Konfiguration der automatischen Kartenregistrierung**

   Ermöglicht es den Benutzern, ihre Transponderkarten selbst zu registrieren.

Aufnahme von MFG in die Secure Access-Datenbank

Jedes MFG muss in der Secure Access-Datenbank registriert werden. Jedem MFG muss ein eindeutiger Name zugewiesen werden. Zudem wird die Netzwerk-IP-Adresse der einzelnen Geräte benötigt.

Im Sinne einer vereinfachten Verwaltung ist dieser Schritt in zwei Unterschritte aufgeteilt: „Eingabe der Geräteparameter“ und „Zuordnung eines Secure Access-Authentifizierungsgeräts zu einem MFG“.

Eingabe der Geräteparameter

1. In Secure Access Manager auf **Devices** (Geräte) klicken.
2. Im Bereich „Settings“ (Einstellungen) in der Geräteliste auf **Add...** (Hinzufügen) klicken.
3. In das dann angezeigte Dialogfeld „Physical Device Summary“ (Physisches Gerät - Überblick) die erforderlichen Informationen eingeben (siehe unten stehende Tabelle).

   Hinweis: Die Felder „Manufacturer“ (Hersteller) und „Model“ (Modell) werden beim ersten Kontakt der Geräts mit der DRE automatisch ausgefüllt. Wenn das Dialogfeld erneut geöffnet wird, sind diese Informationen eingetragen.

Einstellung	Beschreibung
Name	Einen eindeutigen Namen für dieses MFG eingeben. Dieser Name dient zur Identifizierung der Geräts in Secure Access Manager.
Hostname/IP address (Hostname/IP-Adresse)	Entweder die IP-Adresse oder den Hostnamen eingeben. Sicherstellen, dass der Hostname aufgelöst werden kann, wenn die IP-Adresse nicht bekannt ist.
Description (Beschreibung)	Eine Beschreibung eingeben, die anderen Administratoren bei der Geräteidentifizierung hilft, in der Regel ein Name, der sich auf den Standort bezieht. Beispiel: „zweite Etage, PW“.
Authentication Device (Authentifizierungsgerät)	Das Secure Access-Authentifizierungsgerät (nach MAC-Adresse) auswählen, das den Zugriff auf dieses MFG steuern soll. Hinweis: Wird ein Secure Access-USB-Kartenlesegerät verwendet, kein Authentifizierungsgerät zuordnen, sondern den Eintrag „<USB Reader>“ stehen lassen.
Secure Access compatibility (Secure Access-Kompatibilität)	• **MFG with Secure Access capability (MFG mit Secure Access-Kompatibilität):** Diese Option auszuwählen, wenn ein USB-Kartenlesegerät oder ein Xerox-MFG, das Secure Access unterstützt, verwendet wird. Der auf diesem MFG eingerichtete Benutzername des Administrators und das zugehörige Kennwort müssen ebenso eingegeben werden. • **Other type of MFP or printer (MFG oder Drucker anderer Art):** Diese Option auswählen, wenn das Authentifizierungsgerät beim Follow-You-Druck in Verbindung mit einem MFG oder Drucker verwendet wird, das bzw. der Secure Access nicht unterstützt.
Server	Den Namen des Computers eingeben, auf dem die DCE zur Steuerung des MFGs oder Druckers installiert ist.

<table>
<tr><th>Einstellung</th><th>Beschreibung</th></tr>
<tr><td>Initialize Secure Access device (Secure Access-Gerät initialisieren)</td><td>Das Secure Access-Gerät wird im Rahmen der Erstkonfiguration automatisch initialisiert. Wenn das MFG geändert wird, das Secure Access-Gerät durch Klicken auf diese Schaltfläche initialisieren. Mit einem Popup-Fenster wird die erfolgreiche Initialisierung bestätigt.

Hinweis: Mithilfe dieser Schaltfläche kann der Dienst „Release My Documents“ installiert werden. Weitere Einzelheiten siehe Konfiguration des Diensts „Release My Documents“ Seite 40.</td></tr>
<tr><td>Behavior (Ablauf)</td><td>Bei Verwendung des Secure Access-Portmonitors zur Aktivierung des Follow-You-Drucks kann zwischen zwei Freigabeoptionen gewählt werden:
• At assigned control terminal (Am zugewiesenen Kontrollterminal): Der Benutzer muss seine Karte am MFG einlesen lassen, um an dieses Gerät gesendete Dokumente freigeben zu können.
• Release documents from pull group (Dokumente aus einer Gerätegruppe freigeben): Nach der Authentifizierung kann der Benutzer den Anweisungen auf dem Steuerpult folgen, um in der Warteschlange befindliche Dokumente aus einer bestimmten Gerätegruppe auszuwählen. Genauere Informationen siehe Konfiguration des Follow-You-Drucks Seite 31.
Diese Einstellungen haben keine Auswirkung auf die Windows-Portmonitore.</td></tr>
</table>

4. Auf **OK** klicken, um die Einstellungen zu speichern.

   Hinweis: Können auf dem Gerät Zusatzdienste aktiviert werden und wurden im Dialogfeld „Devices“ (Geräte) Änderungen vorgenommen, wird folgende Frage angezeigt:

   - „Do you want to enable Follow-You Printing?“ (Follow-You-Druck aktivieren?) - wenn „Release My Documents“ nicht installiert ist
   - „Do you want to keep Follow-You Printing enabled?“ (Follow-You-Druck aktiviert lassen?) - wenn „Release My Documents“ installiert ist

Zuordnung eines Secure Access-Authentifizierungsgeräts zu einem MFG

Hinweis: Bei Verwendung eines Secure Access-USB-Kartenlesegeräts kann dieser Schritt übersprungen werden.

Wenn ein an das Netzwerk angeschlossenes Authentifizierungsgerät zum ersten Mal eingeschaltet wird, wird das Gerät von der DCE registriert. Das Gerät wird in Secure Access Manager als ein nicht zugeordnetes Secure Access-Authentifizierungsgerät angezeigt. Jedem MFG muss ein bestimmtes Secure Access-Authentifizierungsgerät zugeordnet werden. Mithilfe der bei der Hardware-Einrichtung ausgefüllten Konfigurationsübersicht (siehe Installationshandbuch) die einzelnen Authentifizierungsgeräte den entsprechenden MFG zuordnen.

1. In Secure Access Manager auf **Devices** (Geräte) klicken und das zu konfigurierende MFG auswählen.
2. Im Dialogfeld „Physical Device Summary“ (Physisches Gerät - Überblick) die Dropdown-Liste „Hardware Address“ (Hardware-Adresse) einblenden.
3. Anhand der Konfigurationsübersicht die korrekte MAC-Adresse des Authentifizierungsgeräts, das dieses MFG kontrollieren soll, auswählen.
4. Auf **OK** klicken, um die Änderungen zu speichern.

Einrichtung der Authentifizierungsparameter

Vor dem Import von Benutzerkonten muss der Core Authentification Server (CAS) konfiguriert werden, damit die Konten anhand der primären und sekundären Konten-PINs überprüft werden können. Die PIN-Information verbindet ein Secure Access-Benutzerkonto mit den Informationen auf einer Magnetstreifenkarte.

Bei der primären PIN handelt es sich um eine numerische Zeichenfolge, die den Benutzer eindeutig identifiziert. In der Regel ist dies die Kartennummer. Zur Eingabe der primären PIN lässt der Benutzer einfach seine Karte auslesen.

Wenn eine zusätzliche Sicherheitsstufe bevorzugt wird, kann eine sekundäre PIN aktiviert werden. Wenn diese Option aktiviert wurde, muss der Benutzer zunächst seine Karte einlesen lassen und anschließend am vorderen Steuerpult des MFGs ein zusätzliches Kennwort eingeben. Nur wenn beide Eingaben (die Daten auf der Magnetstreifenkarte und das sekundäre PIN-Kennwort) authentifiziert werden, erhält der Benutzer Zugriff auf das MFG.

1. In Secure Access Manager **Configuration** > **Authentication Device Settings** (Konfiguration > Einstellungen des Authentifizierungsgeräts) auswählen.
2. Im Bereich **Authentication mechanisms** (Authentifizierungsmethoden) mindestens eine Authentifizierungsmethode auswählen:
   - Die Option **Secure Access PINs** nur ausgewählt lassen, wenn ein Secure Access-Druckkonto mit Anmeldedaten verbunden werden soll.
   - Die Option **External user ID and password** (Externe Benutzerkennung und Kennwort) nur aktivieren, wenn Magnetstreifenkarten zur Verifizierung aller Benutzerdaten außerhalb von Secure Access verwendet werden.
   - Die Option **Secure Access PIN with external password** (Secure Access-PIN mit externem Kennwort) aktivieren, wenn Benutzer ihre Karten für die Identifikation durch ein Lesegerät ziehen und zusätzlich ihr Secure Access-Domänenbenutzerkennwort eingeben müssen. Von Secure Access wird in der Datenbank das Vorhandensein eines entsprechenden Kontonamens und dann das Konto anhand der ausgewählten externen Stelle für die Netzwerkanmeldung überprüft.

   Hinweis: Wenn eine externe Authentifizierungsmethode ausgewählt wurde, wird das Feld **Enable secondary prompt** (Sekundäre Eingabeaufforderung aktivieren) automatisch aktiviert. Eine externe Authentifizierung kann nicht erfolgen, wenn das Feld für die sekundäre PIN leer bleibt.
3. Im Bereich **External authorities** (Externe Stellen) nur eine oder mehrere externe Stellen auswählen, wenn eine entsprechende Authentifizierungsmethode festgelegt wurde.
   - Die Option **Windows** auswählen, um Konten anhand der Standard-Windows-Domäne zu überprüfen. Den Domänennamen im Feld **Default domain** (Standarddomäne) angeben.
   - Die Option **NetWare** auswählen, um Konten in einem Standard-NetWare-Kontext zu überprüfen. Den Namen in das Feld **Default context** (Standardkontext) eingeben.

   Hinweis: Die Novell NetWare-Clientsoftware für Windows muss auf dem Core Authentication Server installiert sein, wenn die Überprüfung im Rahmen eines NetWare-Kontexts erfolgen soll.

- Die Option **LDAP** auswählen, um Konten anhand eines LDAP-Servers zu überprüfen. Den LDAP-Servernamen eingeben und aus der Liste einen LDAP-Typ auswählen. Die Option „Force SSL Encryption" (SSL-Verschlüsselung erzwingen) aktivieren, wenn Secure Socket Layer-Verschlüsselung verwendet werden soll.

4. Im Bereich **Card setup** (Karteneinstellung) wie folgt vorgehen:
   a. Die Start- und Enddatenposition in die entsprechenden Felder eingeben. Die von diesen Positionen abgerufenen Daten werden als primäre PIN verwendet.
   b. Auf **<None>** (Keine) neben **HID decoding** (HID-Entschlüsselung) klicken, falls ein Lesegerät für HID-Transponderkarten verwendet wird. Die Authentifizierungsgeräte müssen so konfiguriert werden, dass Karteninformationen in einem Standardformat zurückgegeben werden.

   Einzelheiten zur Eingabe der Entschlüsselungsparameter siehe HID-Entschlüsselung Seite 29.

   c. Die Option **Auto-register primary PINs** (Primäre PINs automatisch registrieren) auswählen, damit Benutzer eine unbekannte Transponderkarte selbst zur künftigen Verwendung registrieren können. Weitere Einzelheiten siehe Automatische Registrierung von Magnetstreifenkarten Seite 29.
5. Im Bereich **Secure Access device prompts** (Secure Access-Geräteeingabeaufforderungen) den Standardtext eingeben, der auf dem MFG-Steuerpult angezeigt werden soll.
   a. Im Feld **Title** (Überschrift) eine Überschrift eingeben, die bei allen Eingabeaufforderungen angezeigt werden soll.
   b. Im Feld **Login prompt** (Anmeldeaufforderung) den Text für die Benutzeranmeldung eingeben. Beispiel: „Bitte zur Anmeldung Karte einlesen lassen."
   c. Die Option **Enable secondary prompt** (Sekundäre Eingabeaufforderung aktivieren), wenn auf dem Display des Xerox-MFG-Steuerpults eine Eingabeaufforderung für einen sekundären PIN-Code (oder ein Kennwort) angezeigt werden soll.
   d. Die Option **Enable release all jobs prompt** (Eingabeaufforderung für die Freigabe aller Aufträge aktivieren) aktivieren, wenn auf dem Display des Xerox-MFG-Steuerpults eine Eingabeaufforderung angezeigt werden soll, in der der Benutzer gefragt wird, ob er alle in der Warteschlange befindlichen Aufträge für den Druck freigeben möchte.
6. Im Bereich **SNMP** die **Get-** und **Set-Communitynamen** eingeben.

   Hinweis: Wenn die Standardnamen in Secure Access geändert werden, die gleiche Namensänderung auf allen physischen Geräten wiederholen, damit die SNMP-Kommunikation funktioniert. Informationen zur Änderung dieser Einstellungen enthält die MFG-Dokumentation.
7. In das Feld **JBA Account ID** die JBA-Konto-ID eingeben, wenn Secure Access mit einer JBA-Kostenzählungsanwendung eines Drittanbieters genutzt werden soll.
8. In das Feld **Job expiry time (in hours)** (Auftragsablaufzeit in Stunden) die Zeit in Stunden eingeben, nach der in der Warteschlange befindliche Aufträge gelöscht werden sollen. Die Standardeinstellung ist eine Stunde.
9. Werden im Netzwerk nicht die Standard-SNMP-Communitynamen („public" für Lesezugriff, „private" für Schreibzugriff) verwendet, die verwendeten Namen in die entsprechenden Felder im Dialogfeld eingeben. Auf allen Geräten müssen die gleichen Namen verwendet werden.

   Hinweis: Werden keine Communitynamen angegeben, werden Gerätetypen bei der Erstellung neuer Ports nicht automatisch ermittelt. Allerdings können Ports weiterhin unter manueller Angabe der Verbindungsdaten erstellt werden.
10. Auf **OK** klicken, um die Einstellungen zu speichern.

HID-Entschlüsselung

Die HID-Verschlüsselung wie folgt konfigurieren:

1. In Secure Access Manager **Configuration** > **Authentication Device Settings** (Konfiguration > Einstellungen des Authentifizierungsgeräts) auswählen.
2. Im Bereich „Card Setup“ (Karteneinstellung) auf **<None>** (Keine) neben **HID decoding** (HID-Entschlüsselung) klicken.
3. Im Dialogfeld **HID decoding** (HID-Entschlüsselung) wie folgt vorgehen:
   - Ist die Verschlüsselung bekannt, die folgende HID-Kartenverschlüsselungsinformation eingeben. Ist die Verschlüsselung nicht bekannt, den HID-Händler nach dem auf den Transponderkarten verwendeten Verschlüsselungstyp fragen.
   - Für den Fall, dass keine Facility-Code-Informationen extrahiert werden müssen, nur die Option **ID code** (ID-Code) aktivieren. Wenn Facility-Code und ID-Code extrahiert werden müssen, beide Optionen aktivieren.

   a. In das Feld **Facility Start** (Facility-Start) die Position im Raw-Bitstream (0-basierend, von links nach rechts, inklusiv) eingeben, ab der der Facility-Code beginnt.

   b. In das Feld **Facility End** (Facility-Ende) die Position im Raw-Bitstream (0-basierend, von links nach rechts, inklusiv) eingeben, wo der Facility-Code endet.

   c. In das Feld **Facility Width** (Facility-Breite) die Anzahl der Dezimalstellen für den Facility-Teil des Werts angeben, den das Authentifizierungsgerät ausgibt. Bei Bedarf werden die Zahlen auf der linken Seite mit Nullen aufgefüllt. Wenn am Standort oder beim HID-Kartenformat kein Facility-Code verwendet wird oder wenn dieser nicht als Teil des Kartenwerts zurückgemeldet werden muss, eine Breite von 0 eingeben, um das Extrahieren der Facility-Nummer zu deaktivieren.

   d. In das Feld **ID Start** (ID-Start) die Position im Raw-Bitstream (0-basierend, von links nach rechts, inklusiv) eingeben, an der der ID-Code beginnt.

   e. In das Feld **ID End** (ID-Ende) die Position im Raw-Bitstream (0-basierend, von links nach rechts, inklusiv) eingeben, an der der ID-Code endet.

   f. In das Feld **ID Width** (ID-Breite) die Anzahl der Dezimalstellen für den ID-Code-Teil des Werts angeben, den das Authentifizierungsgerät ausgeben wird. Bei Bedarf werden die Zahlen auf der linken Seite mit Nullen aufgefüllt. Das Authentifizierungsgerät liefert bei jedem Einlesen der Karte einen einzelnen Wert zurück; dabei handelt es sich um den entschlüsselten Facility-Code, dem die entschlüsselte ID folgt.

   g. Auf **OK** klicken, um die Einstellungen zu speichern.

Automatische Registrierung von Magnetstreifenkarten

Diese Option in Secure Access aktivieren, damit Benutzer ihre Magnetstreifenkarten selbst registrieren können.

1. In Secure Access Manager **Configuration** > **Authentication Device Settings** (Konfiguration > Einstellungen des Authentifizierungsgeräts) auswählen.
2. Die Option **Auto-register primary PINs** (Primäre PINs automatisch registrieren) im Bereich **Card Setup** (Karteneinstellung) auswählen.
3. Auf **OK** klicken, um die Änderungen zu speichern.

Wenn ein Benutzer versucht, eine nicht registrierte Karte auslesen zu lassen, muss er sich mit gültigen Benutzeranmeldeinformationen (Benutzerkennung und Kennwort) beim MFG anmelden. Die automatische Registrierung setzt voraus, dass die Benutzeranmeldeinformationen bereits im CAS vorhanden sind.

Nach der Registrierung werden die Kontoinformationen des Benutzers beim nächsten Auslesen der Karte automatisch der Karte zugeordnet. Der Benutzer kann sich anmelden, ohne seine Benutzeranmeldeinformationen manuell einzugeben. Gegebenenfalls wird der Benutzer aufgefordert, eine sekundäre PIN einzugeben (sofern konfiguriert).

> Hinweis: Wenn die Option **Secure Access PIN with external password** (Secure Access-PIN mit externem Kennwort) beim Konfigurieren der automatische Kartenregistrierung ausgewählt wurde, wird die Secure Access-PIN von den Magnetkartendaten überschrieben, sobald die Karte authentifiziert und registriert ist. Die Secure Access-PIN kann nicht mehr zur Anmeldung verwendet werden.

Konfiguration des Follow-You-Drucks

Beim Follow-You-Druck kann ein Benutzer einen Druckauftrag an ein bestimmtes MFG senden, sich aber über ein anderes MFG authentifizieren und anschließend eine Liste der in einer gesicherten Warteschlange abgelegten Aufträge anzeigen. Der Benutzer kann den Auftrag dann auf das MFG, auf dem er sich authentifiziert hat, „ziehen", selbst wenn es sich nicht um das ursprünglich ausgewählte Ausgabegerät handelt.

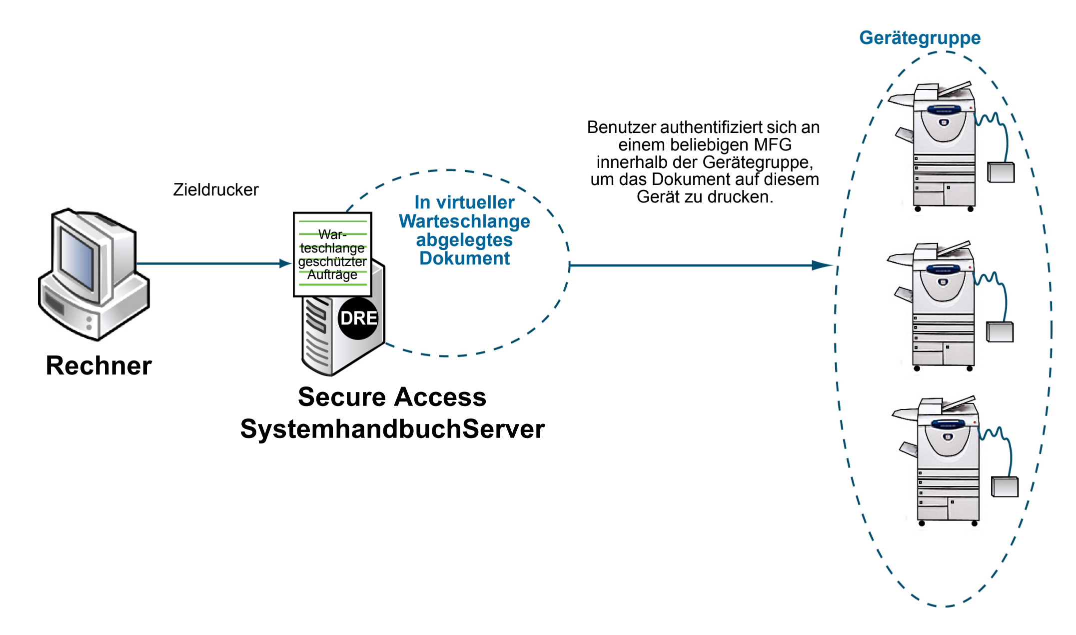


Abbildung 4-1: Follow-You-Druck

Zur Konfiguration des Follow-You-Drucks sind zwei Schritte erforderlich:

1. Die Verwendung des Secure Access-Portmonitors, um die Konfiguration zwischen Druckserver und allen kontrollierten MFG ermöglichen. Die vorhandenen Windows-Ports können in Secure Access-Ports konvertiert werden. Der Portmonitor fängt alle an Geräte innerhalb einer Gerätegruppe gesendeten Dokumente ab und hält sie in der gesicherten Warteschlange, bis sie durch den authentifizierten Benutzer freigegeben werden. Weitere Einzelheiten siehe Konvertierung von Ports für den Secure Access-Portmonitor Seite 32.
2. Gerätegruppen in Secure Access Manager erstellen. Siehe Erstellung von Gerätegruppen Seite 33.

Sollen Benutzer geschützte Aufträge in Warteschlangen direkt am MFG anzeigen können, auf diesem den Dienst „Release My Documents" aktivieren. Weitere Einzelheiten siehe Konfiguration des Diensts „Release My Documents" Seite 40.

Konvertierung von Ports für den Secure Access-Portmonitor

Secure Access verwendet spezielle Ports, um den Follow-You-Druck zu ermöglichen. Jedes Gerät, das Mitglied einer Gerätegruppe sein soll, muss einen Secure Access-Portmonitor nutzen. Wenn vorhandene Geräte bereits für die Verwendung von Windows-Ports eingerichtet wurden, können sie problemlos konvertiert werden.

1. Dafür sorgen, dass die zu konvertierenden Geräte eingeschaltet, an das Netzwerk angeschlossen und für den Druck konfiguriert sind.
2. Über den Windows-**Arbeitsplatz** zum Installationsverzeichnis von Secure Access navigieren.
3. Den Ordner **Tools** öffnen und auf **SAPrinterConversionWizard.exe** doppelklicken.
4. Im Begrüßungsbildschirm des „Printer Conversion Wizard“ (Assistent für die Druckerkonvertierung) auf „Next“ (Weiter) klicken.
5. Unter **Print server location** den Druckserver-Speicherort auswählen.

   Wenn der Druckserver (DRE) sich auf dem lokalen Gerät befindet, die Option **Local Machine** (Lokales Gerät) auswählen. Andernfalls die Option **Remote server** (Remote-Server) wählen.
6. Die Option **Convert printers to use the Secure Access Port Monitor** (Drucker für die Nutzung des Secure Access-Portmonitors konvertieren) auswählen. Anschließend auf **Next** (Weiter) klicken.
7. In der Liste **Convert Printers** (Drucker konvertieren) Drucker auswählen oder löschen. Anschließend auf **Next** (Weiter) klicken.
8. Auf **Finish** (Fertig stellen) klicken, um die Konvertierung abzuschließen.

Erstellung einer Druckerwarteschlange mit einem Secure Access-Portmonitor

Je nach Druckerhardware werden möglicherweise mehrere Ports benötigt, die den Secure Access-Portmonitor auf einem Druckserver verwenden. Es kann eine neue Druckerdefinition konfiguriert werden, die den Secure Access-Portmonitor nutzt.

1. In Windows den **Druckerinstallations-Assistenten** aufrufen.
2. Den Anweisungen zum Hinzufügen eines lokalen Druckers und Erstellen eines neuen Ports folgen.
3. Bei Aufforderung **Secure Access Port** als zu erstellenden Porttyp wählen und auf „Next“ (Weiter) klicken. Das Fenster „Add Secure Access Printer Port Wizard“ (Assistent zum Hinzufügen eines Secure Access-Druckerports) wird angezeigt. Bestätigen, dass der Drucker eingeschaltet, an das Netzwerk angeschlossen und korrekt konfiguriert ist.
4. Auf **Next** (Weiter) klicken und aus der Dropdown-Liste **Device Type** (Gerätetyp) **Physical printer** (Physischer Drucker) auswählen.
5. In das Feld **Printer name or IP address** (Druckername oder IP-Adresse) einen Druckernamen oder eine IP-Adresse eingeben.
6. Der Assistent stellt basierend auf dem Druckernamen oder der IP-Adresse einen **Portnamen** zur Verfügung. Bei Bedarf kann dieser Name manuell geändert werden.
7. Auf **Next** (Weiter) klicken, um mit der Konfiguration weiterer Portoptionen fortzufahren. Das Fenster „Port Configuration“ (Portkonfiguration) wird angezeigt. Die Anzeige **Detected device information** (Ermittelte Geräteinformationen) wird automatisch eingeblendet, wenn der Assistent diese Daten vom Drucker abrufen kann.

8. Festlegen, ob für diesen Port standardmäßige oder benutzerdefinierte Einstellungen verwendet werden sollen.

   Bei Auswahl der Option **Use custom settings** (Benutzerdefinierte Einstellungen verwenden):

   a. Bei Auswahl der Option **Raw port communication** (Raw Port-Kommunikation), die TCP-Portnummer eingeben und festlegen, ob die Verbindung über den Portmonitor offen gehalten werden soll.
   b. Bei Auswahl von **LPR** den Namen der Druckerwarteschlange auf dem physischen Gerät eingeben (beispielsweise PORT1).
   c. Bei Auswahl der Option **Specific device** (Spezifisches Gerät) in den Dropdown-Listen **Manufacturer** (Hersteller) und **Model** (Modell) jeweils eine Option wählen. Basierend auf dieser Auswahl nutzt das Gerät die zugehörigen Standard-Kommunikationsparameter.
9. Auf **Next** (Weiter) klicken und unter **Physical device name** (Name des physischen Geräts) den Namen für das physische Gerät angeben. Dies ist der Name für das Gerät, der in Secure Access angezeigt wird.
10. Die Angaben für diesen neuen Port und die Geräteregistrierung überprüfen und anschließend auf **Finish** (Fertig stellen) klicken, um den Assistenten für das Hinzufügen eines Secure Access-Druckerports zu schließen. Wenn die Einstellungen korrigiert werden müssen, auf **Back** (Zurück) klicken. Nach dem Beenden des Assistenten für das Hinzufügen eines Secure Access-Druckerports wechselt die Anzeige wieder zurück in den Windows-Druckerinstallationsassistenten.
11. Die restlichen Schritte im Druckerinstallationsassistenten ausführen. Um eine Testseite zu drucken, im nächsten Dialogfeld auf **Ja** klicken.
12. Die Angaben für den Windows-Drucker bestätigen und auf **Fertig stellen** klicken, um den Assistenten zu beenden. Bei Bedarf auf **Zurück** klicken, um notwendige Korrekturen vorzunehmen.

Erstellung von Gerätegruppen

Die zu erstellenden Gerätegruppen sollten an die Anforderungen des Unternehmens angepasst werden. Beispielsweise können kompatible Geräte nach physischem Standort, nach Abteilung, nach Hersteller usw. gruppiert werden. Es können auch Gerätegruppen erstellt werden, die eine Auswahl von Geräten eines einzelnen Druckservers enthalten.

Der für die Gerätegruppe gewählte Gerätetreiber muss mit allen Geräten dieser Gruppe kompatibel sein. Wenn ein für die Ausgabe auf einem bestimmten MFG generierter Druckauftrag einwandfrei auf einem anderen MFG gedruckt werden soll, muss sichergestellt werden, dass dieser andere Drucker alle Druckbefehle versteht, die im Datenstrom des Treibers enthalten sind.

1. In Secure Access Manager auf die vorhandenen MFG klicken, die derselben Gerätegruppe zugeordnet werden sollen.
2. Im Dialogfeld „Physical Device Summary“ (Physisches Gerät - Überblick) die Option **Release documents from pull group** (Dokumente aus Gerätegruppe freigeben) auswählen. Den Namen der Gerätegruppe eingeben (dies kann ein beliebiger Name sein, der sinnvoll erscheint). Anschließend auf **OK** klicken, um die Änderungen zu übernehmen.

   Hinweis: Nur bei der ersten Verwendung muss der Name der Gerätegruppe eingegeben werden. Anschließend erscheint er automatisch in der Liste.
3. Die Schritte 1 und 2 wiederholen, um Geräte auszuwählen und andere Gerätegruppen zu erstellen.

Import und Synchronisierung von Benutzerkonten

Um die Authentifizierung zu ermöglichen, müssen Benutzerkonten erstellt werden, die den auf der Magnetstreifenkarte genutzten Attributen entsprechen. Wenn ein Benutzer seine Karte einlesen lässt, leitet das Authentifizierungsgerät diese Zugriffsanforderung an die DCE weiter. Die DCE wiederum übermittelt die von der Karte eingelesenen Daten an den CAS. Wenn der CAS ein Benutzerkonto mit Attributen, die denen auf der Karte entsprechen, findet, wird die Sperrung des MFGs aufgehoben, so dass der Benutzer den Fax-, Scan-, Kopier- oder Druckauftrag freigeben kann.

In Secure Access stehen drei Methoden für den Import von Benutzerkonten zur Verfügung:

- Import (und optional Synchronisieren) von Konten mit Active Directory
- Import von Benutzerkonten aus einer CSV-Datei
- Manuelle Erstellung von Konten in Secure Access Manager

Verwendung von Active Directory für den Import vorhandener Benutzerkonten

Ist ein Active Directory-Server vorhanden, können die Konteninformationen, die importiert und synchronisiert werden sollen, ausgewählt werden. Eine Synchronisierung vermindert den Verwaltungsaufwand und ermöglicht die automatische Aktualisierung von Konten.

Durch die Ausführung der nachstehend beschriebenen Schritte wird ein Hintergrundprozess gestartet. In Secure Access Manager auf das Tool „Users“ (Benutzer) klicken, um das Ergebnis des Hintergrundprozesses anzuzeigen. Die Benutzerliste wird automatisch ausgefüllt, wenn der Prozess abgeschlossen ist.

> Hinweis: Die Secure Access-Dienste müssen von einem Domänenkonto mit Zugriff auf das entsprechende Active Directory gestartet werden. Es muss eine Anmeldung als Domänenadministrator aktiv sein. Wenn die Dienste unter dem Konto des lokalen Administrators gestartet werden, schlägt die Active Directory-Synchronisierung fehl.

Es ist wichtig, die Optionen im Dialogfeld „Active Directory Synchronization“ (Active Directory-Synchronisierung) in der korrekten Reihenfolge auszuwählen. Die nachfolgenden Schritte daher genau befolgen.

1. In Secure Access Manager auf **Configuration** > **Active Directory Synchronization** (Konfiguration > Active Directory-Synchronisierung) klicken.
2. Im Bereich **Domain controllers** (Domänencontroller) auf **Add** (Hinzufügen) klicken. Ein Domänencontroller ist ein Server, der Mitglied-Computern den Zugriff auf Active Directory ermöglicht. Den Namen des Controllers in das Feld eingeben.

3. Im Bereich **Containers** (Container) auf **Add** (Hinzufügen) klicken. Ein Container ist ein Ordner in der Active Directory-Baumstruktur, der Benutzer, Gruppen oder Computer enthält.

ACHTUNG: Sicherstellen, dass die ausgewählten Organisationseinheiten-Container nur Benutzerkontendaten enthalten. Wenn die Organisationseinheiten andere Daten enthalten (z. B. System- oder Kontaktdaten), kommt es zu unerwarteten Ergebnissen. Möglicherweise müssen spezielle Organisationseinheiten-Container für Import- und Synchronisierungszwecke erstellt werden.

4. Unter **Synchronization interval** (Synchronisierungsintervall) einstellen, wie häufig die Secure Access-Datenbank mit dem angegebenen Active Directory synchronisiert werden soll. Der Mindestwert für das Synchronisierungsintervall liegt bei 15 Minuten.
5. Unter **Active Directory updates to be applied** (Anzuwendende Active Directory-Updates) die Optionen **Adds** (Hinzufügungen), **Deletes** (Löschungen) oder **Changes** (Änderungen) aktivieren oder deaktivieren, um festzulegen, welche Active Directory-Konten Secure Access empfängt und während der nachfolgenden Synchronisierungen in die Kontendatenbank übernimmt.

   Es besteht die Möglichkeit, hinzugefügte oder geänderte Benutzerkonten zu importieren oder inaktive Konten aus der Secure Access-Datenbank zu löschen. Wenn diese Einstellungen mit den Standardwerten beibehalten werden, ist gewährleistet, dass die Konten im Einklang mit dem Active Directory-Server verwaltet werden.
6. Die Attribute unter **Assign Values from Active Directory** (Werte aus Active Directory zuweisen) sparen Zeit und Mühe, indem bestimmte Attribute allen Benutzern innerhalb des ausgewählten Containers zugewiesen werden. Hinweis: Hier nicht den Feldnamen, sondern den Active Directory-Attributnamen eingeben. Obwohl individuelle Benutzerkonten später aktualisiert werden können, diese Attribute vor dem Import wählen, um die Kontenerstellung zu beschleunigen.

   Die Attribute **Primary PIN** (Primäre PIN) und **Secondary PIN** (Sekundäre PIN) ordnen die auf dem Active Directory-Server vorgefundenen numerischen PIN-Werte den Feldern „Primary PIN“ (Primäre PIN) und „Secondary PIN“ (Sekundäre PIN) in Secure Access zu. Die Option „Secondary PIN“ (Sekundäre PIN) aktivieren, wenn diese Felder importiert werden sollen. Der Benutzer kann diese Felder am MFG-Steuerpult ausfüllen (eine sekundäre Eingabeaufforderung ist wie ein Kennwort, das einen zusätzlichen Sicherheitsaspekt einbringt), wenn die sekundäre Eingabeaufforderung unter **Configuration** > **User Authentication Device Settings** (Konfiguration > Benutzereinstellung für Authentifizierungsgerät) aktiviert wurde. Den Attributnamen für die Felder „PIN1“ (in der Regel die Kartennummer) und „PIN2“, die auf dem Active Directory-Server verwendet werden, eingeben.

   Die Attribute **Primary PIN** (Primäre PIN) und **Secondary PIN** (Sekundäre PIN) können auch E-Mail-Adressen zuordnen.
7. Auf **Import** (Importieren) klicken, um den ersten Import unmittelbar zu starten. Der Import erfolgt im Hintergrund und kann abhängig von der Größe des zu importierenden Active Directory einige Minuten dauern.
8. Durch Klicken auf **OK** kann das Dialogfeld geschlossen werden. Auch wenn das Dialogfeld geschlossen wurde, läuft der Import im Hintergrund weiter.
9. Nach einigen Minuten die Ansicht von Secure Access Manager aktualisieren. Anschließend anhand der Benutzerliste überprüfen, ob der Import der Benutzerkonten erfolgreich war. Außerdem die Eigenschaften eines Benutzerkontos öffnen, um zu prüfen, ob auch diese Einstellungen korrekt sind.

Import von Benutzerkonten aus einer Flatfile

Mit dem Dienstprogramm **SACmd.exe** können Benutzerkonten aus einer Flatfile hinzugefügt, gelöscht, modifiziert und abgefragt werden.

> Hinweis: Bei dieser Methode handelt es sich um einen einmaligen Import, bei dem die Daten über den Import hinaus nicht synchronisiert werden.

Dieses Dienstprogramm wird standardmäßig auf dem Authentifizierungsserver im Verzeichnis **Programme** > **Xerox** >**Secure Access** > **Tools** installiert.

Befehle müssen in folgendem Format eingegeben werden:

```
SACmd  -s(Server) (Aktion) (Objektkennung)| [(Optionen)]
Beispiel: -sTestserver add user1 "Britta Muster" brittam@firma.de pin1 pin2
```

Den Befehl mit einer Batchdatei ausführen:

```
SACmd  -s(Server) -f(Batchdatei)
```

SACmd-Batchdatei-Prozess

SACmd verfügt über einen Batchmodus und akzeptiert CSV-Dateien als Batchdateien (eine Datei pro Server). Im Batchbetrieb können alle Befehle mit Ausnahme des Abfragebefehls (query) verarbeitet werden.

> Hinweis: Die CSV-Datei in den Ordner **Secure Access** > **Tools** kopieren.

```
[Secure Access\Tools_Dateipfad]\SACmd –s(Server) –f Batchdateiname.csv
```

CSV-Dateiformat: `(Aktion), (Objektkennung)|All,   [(Details)]`

In Klammern ( ) stehende Befehlszeilenparameter sind obligatorisch. Parameter in eckigen Klammern [ ] sind optional. Nachstehende Tabelle als Referenz für die Eingabe der Parameter verwenden.

Parameter	Variablen
Server	Der Name oder die IP-Adresse des CAS
Aktion	Die für das Konto zu ergreifende Aktion angeben. Zur Auswahl stehen: • add - Benutzer hinzufügen • delete - Benutzer löschen • query - Datenbank abfragen • modify - Objektattribut modifizieren

Parameter	Variablen
Objektkennung	Wendet die Aktion nur auf die entsprechende Objektkennung an. Objektkennungen, die Leerzeichen enthalten (wie zum Beispiel „Britta Muster“), in Anführungszeichen setzen.
Optionen für Parameter „Aktion“	Zusätzliche Werte angeben. Leere Werte und Detailwerte, die Leerzeichen enthalten, in Anführungszeichen setzen. Zahlen mit einem Punkt als Dezimaltrennzeichen eingeben. Bei der Aktion „modify“ für obligatorische Felder, die nicht geändert werden sollen, „!“ eingeben. (user_ID): Benutzerkennung (user_name): Benutzername (email): E-Mail-Adresse

Add

Mit **add** (Hinzufügen) können Benutzerkonten hinzugefügt werden. Erfordert Werte bis zum und einschließlich des letzten erforderlichen Felds.

Benutzer hinzufügen:

```
add(Benutzerkennung) [(Benutzername) (E-Mail-Adresse) (primäre PIN)
(sekundäre PIN)]
```

Beispiel:

```
SACmd -sMeinServer add BrittaM “Britta Muster” “brittam@firma.de” 123
Kennwort
```

Delete

Mit **delete** (Löschen) können Benutzerkonten gelöscht werden.

Benutzerkonto löschen:

```
delete (Benutzerkennung)
```

Beispiel:

```
SACmd -sMeinServer delete BrittaM
```

Modify

Mit „modify“ (Ändern) können Einstellungen der Benutzerdatenbank geändert werden. Erfordert Werte bis zum und einschließlich des letzten erforderlichen Felds.

Benutzer modifizieren:

```
modify (Benutzerkennung) [(Benutzername) (E-Mail-Adresse) (primäre PIN)
(sekundäre PIN)]
```

Beispiel: Die E-Mail-Adresse von Benutzer brittam ändern und die restlichen Daten beibehalten:

```
SACmd -sMeinServer modify brittam! brittam@neuefirma.de
```

Manuelle Kontoerstellung

Mit Secure Access Manager können bei Bedarf individuelle Benutzerkonten hinzugefügt werden.

1. Zunächst die Option „Users“ (Benutzer) auswählen, dann mit der rechten Maustaste im Bereich „Settings“ (Einstellungen) klicken und aus dem Menü die Option **Add User** (Benutzer hinzufügen) wählen.
2. Im Dialogfeld „User Properties“ (Benutzereigenschaften) die erforderlichen Informationen angeben (wie in nachstehender Tabelle aufgeführt).

Feld	Beschreibung
User ID (Benutzerkennung)	Die in der Datenbank verzeichnete ID zur Verfolgung des Benutzerkontos.
Full Name (Vollständiger Name)	Der vollständige Name des Benutzers: Einen vollständigen Namen eingeben, über den der Benutzer in Account Manager oder Department Manager leichter identifiziert werden kann. Dieser Name erscheint auch in Kontenaufstellungen und Berichten.
Email address (E-Mail-Adresse)	E-Mail-Adresse des MFGs, beispielsweise für die Scanausgabe in E-Mails.
Primary PIN (Primäre PIN)	Die primäre PIN ist in der Regel mit der Kartennummer gleichzusetzen.
Secondary PIN (Sekundäre PIN)	Die sekundäre PIN wird als Kennwort verwendet. Der Benutzer muss diese PIN nach dem Einlesen seiner Magnetstreifenkarte am MFG-Steuerpult eingeben, um sich zu authentifizieren.
Confirm Secondary PIN (Sekundäre PIN bestätigen)	Die sekundäre PIN zur Bestätigung des Kennworts erneut eingeben.

Überwachung von Authentifizierungsereignissen

Secure Access zeichnet jedes Authentifizierungsereignis in der Secure Access-Datenbank auf. Es ist möglich, für jedes beliebige Datum ein Authentifizierungsprotokoll zu generieren und den Verlauf von nachstehenden Ereignissen zu verfolgen:

- Authentifizierungsfehler
- Beginn der Sitzung (erfolgreiche Authentifizierung)

Jedes protokollierte Ereignis enthält folgende Informationen:

- IP-Adresse der Quelle
- Primäre PIN
- Überprüfungsergebnis
- Servertyp
- Benutzername
- E-Mail-Adresse
- Servername

Zur Anzeige eines Authentifizierungsprotokolls in Secure Access Manager auf **Authentication log** (Authentifizierungsprotokoll) klicken und mit der rechten Maustaste auf **View log by date** (Protokoll nach Datum anzeigen) klicken. Ein Datum auswählen und dann auf **OK** klicken.

Konfiguration des Diensts „Release My Documents“

Ist der Dienst „Release My Documents“ installiert, so wird am MFG die gleichnamige Option angezeigt. Über diese Option kann der Benutzer seine Aufträge in der Druckwarteschlange aufrufen. Diese kann er dann nach Bedarf auswählen und zum Druck freigeben oder löschen.

> Hinweis: Der Dienst kann nur aktiviert werden, wenn auch Follow-You-Druck eingerichtet ist. Weitere Einzelheiten siehe Konfiguration des Follow-You-Drucks Seite 31.

Ist „Release My Documents“ nicht installiert, kann der Benutzer am MFG keine einzelnen Aufträge zur Freigabe auswählen. Stattdessen kann er vorgeben, dass alle Aufträge auf dem Druckserver direkt nach der Authentifizierung freigegeben werden.

Wird ein Benutzer authentifiziert, erhält die DCE die Daten des Benutzers und ruft die Liste sämtlicher Aufträge dieses Benutzers, die sich in der Warteschlange befinden, vom DRE-Druckserver ab. Diese werden dann in der Anzeige „Release My Documents“ am MFG angezeigt.

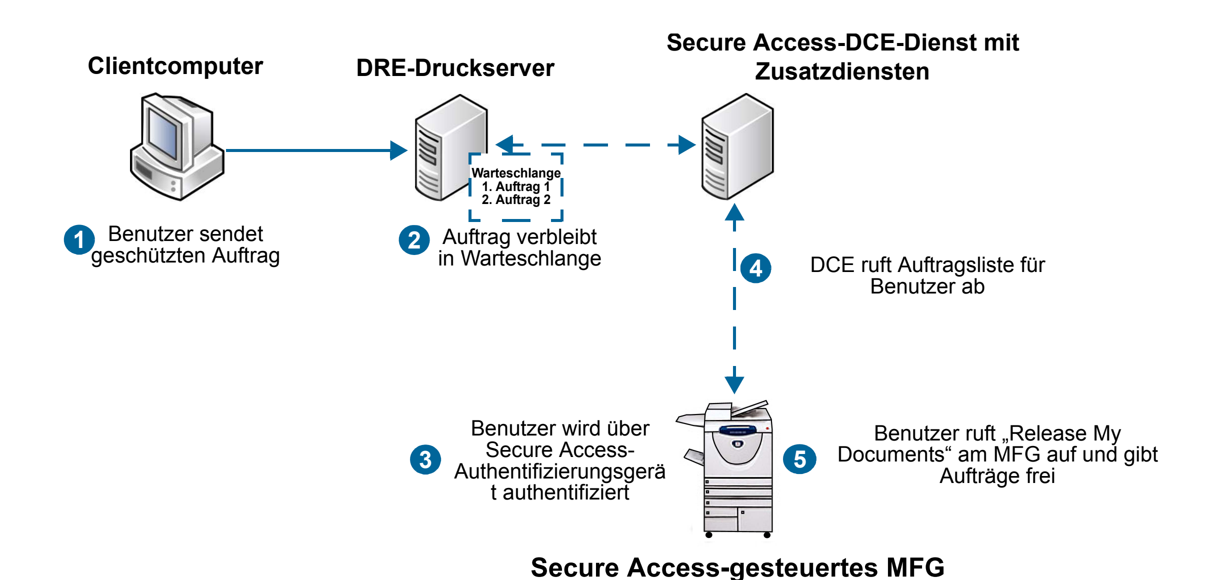


Abbildung 4-2: Release My Documents-Architektur

Aktivierung des Diensts „Release My Documents“ auf einem MFG

Werden in Secure Access Manager neue Geräte eingerichtet, erscheint beim Klick auf „OK“ im Dialogfeld „Devices“ (Geräte) die Frage, ob der Dienst „Release My Documents“ installiert werden soll. Weitere Einzelheiten siehe Eingabe der Geräteparameter Seite 25.

Hinweis: Die Installation dieses Diensts ist optional. Wird er nicht installiert, muss der Benutzer nach der Authentifizierung alle Aufträge auf einmal freigegeben.

Zur Aktivierung des Diensts auf einem Gerät, das bereits in Secure Access Manager konfiguriert ist, folgende Schritte durchführen:

1. In Secure Access Manager auf **Devices** (Geräte) klicken.
2. Das gewünschte Gerät auswählen.
3. Im Dialogfeld "Physical Device Summary" (Physisches Gerät - Überblick) auf die Schaltfläche **Initialize Secure Access device** (Secure Access-Gerät initialisieren) klicken.
4. Die Frage „Do you want to enable Follow-You printing?“ (Follow-You-Druck aktivieren?) mit einem Klick auf **Ja** beantworten.

   Es wird nun im Hintergrund eine Exe-Datei ausgeführt, die den DCE-Dienst aktualisiert und den Dienst „Release My Documents“ auf dem MFG aktiviert.

Zur Überprüfung des Installationserfolgs die Betriebsartentaste auf dem MFG drücken. Bei einwandfreier Installation wird die Schaltfläche **Release my documents** angezeigt. Je nach Gerätemodell muss für den Zugriff auf diesen Dienst eventuell zunächst die Schaltfläche **Zusatzdienste** angetippt werden.

War die Installation nicht erfolgreich, wird eine Schaltfläche mit der Aufschrift **Servicex** (wobei x für eine Zahl steht, z. B. Service4 oder Service5) angezeigt. Zur Lösung dieses Problems siehe Fehlerbehebung beim Dienst „Release My Documents“ Seite 50.

Einsatz von „Release My Documents“

In der nachfolgenden Abbildung wird der Einsatz des Diensts „Release My Documents“ dargestellt. Nach Übermittlung des Druckauftrags meldet sich der Benutzer über ein Secure Access-Authentifizierungsgerät bei einem Secure Access-gesteuerten MFG an und ruft seine geschützten Aufträge über die Option **Zusatzdienste** > **Release My Documents** auf.

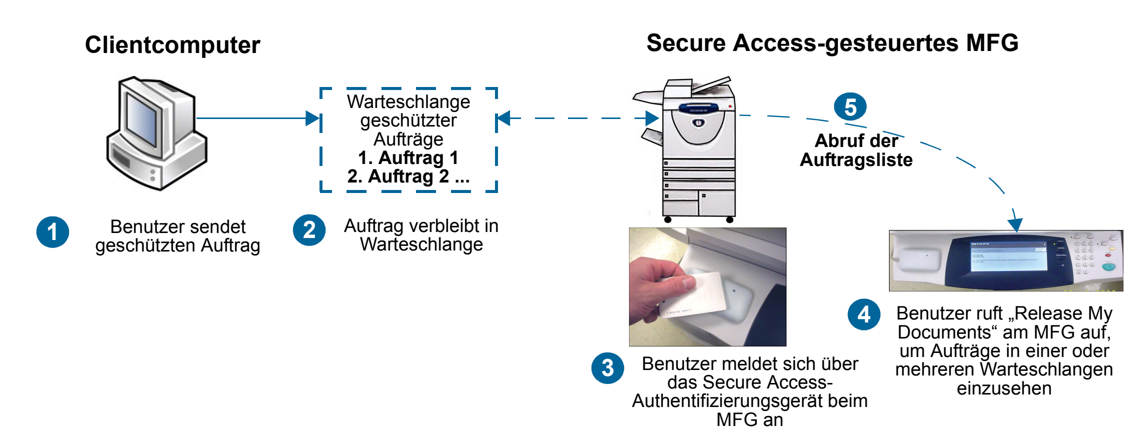


Abbildung 4-3: Einsatz von „Release My Documents“

Anhänge



Themen dieses Kapitels:

Zugriffsberechtigungen für die Verzeichnissynchronisierung

Mit dem Tool **SAModifyDeletedContainerSecurity.exe** werden die administrativen Zugriffsberechtigungen auf den Container mit den gelöschten Objekten in Windows Active Directory geändert, so dass Secure Access während der Verzeichnissynchronisierungen auf die Objekte zugreifen kann.

Standardmäßig besitzen nur Active Directory-Administratoren die erforderliche Zugriffsberechtigung. Das Windows-Konto, das Secure Access ausführt, benötigt diese Zugriffsberechtigung, wenn gelöschte Konten zwischen Active Directory und Secure Access synchronisiert werden sollen.

Zum Ausführen dieses Befehls ist eine Anmeldung als Active Directory-Administrator erforderlich.

Weitere Informationen zur Konfiguration von Active Directory-Synchronisierungsoptionen siehe Verwendung von Active Directory für den Import vorhandener Benutzerkonten Seite 34.

Standardmäßig wird dieses Dienstprogramm auf dem CAS im Verzeichnis **Programme** > **Xerox** > **Secure Access** > **Tools** installiert.

Befehle müssen in folgendem Format eingegeben werden:

```
SAModifyDeletedContainerSecurity.exe (-s server) [-p | {-r} -a accountname]
```

In Klammern ( ) stehende Parameter sind obligatorisch. Parameter in eckigen Klammern [ ] sind optional.

Parameter	Beschreibung
-s server	Servername des Active Directory-Domänencontrollers
-p	Zeigt die aktuellen Berechtigungen auf den Container an
-r	Entfernt die Zugriffsberechtigungen für das angegebene Konto
-a accountname	Konto, dem der Zugriff auf den Container gewährt werden soll; die Zugriffsberechtigung wird entzogen, wenn dies mit der Option -r angegeben wird.

Rücksetzung von Authentifizierungsgeräten

Das Authentifizierungsgerät mit dem Bypass-Schlüssel auf die Standardeinstellungen zurücksetzen. Dieser Schlüssel wurde mit dem Gerät geliefert und sollte an einem sicheren Ort aufbewahrt werden.

1. Sicherstellen, dass das Gerät eingeschaltet ist.
2. Den Bypass-Schlüssel in das Schlüsselloch einführen.
3. Den Schlüssel mit einer Viertelumdrehung in Richtung des eigenen Körpers drehen.
4. Den Schlüssel zurück in die Ausgangsposition drehen.
5. Den Schlüssel abziehen.

   Hinweis: Das Gerät gibt in Abständen von 10 Sekunden ein Tonsignal aus, wenn der Schlüssel vor dem Abziehen nicht in seine ursprüngliche Position zurückgedreht wurde.

Portzuweisungen

Secure Access kommuniziert über folgende Ports:

Komponente	Port
CAS	TCP 2910
DRE	TCP 2938
DCE	TCP 1824, TCP 2939, UDP 2613
Secure Access-Authentifizierungsgerät	TCP 1234

Bei der Installation von Secure Access werden diese Ports automatisch geöffnet. Wenn jedoch die Einstellungen der Windows-Firewall berücksichtigt werden müssen, können die Ports auf jedem Rechner, auf dem eine Secure Access-Serverkomponente implementiert wurde, in die Liste der vertrauenswürdigen Ports aufgenommen werden.

Fehlerbehebung

Im Falle eines Fehlers zunächst die unten aufgeführten Maßnahmen ergreifen und erst dann den Kundendienst anfordern, wenn ein Fehler sich so nicht beheben lässt.

	Symptom	Anweisungen
1	LED am Lesegerät leuchtet nicht	**Authentifizierungsgerät**: Eine nicht leuchtende LED auf dem Kartenlesegerät weist auf fehlenden Strom hin. Authentifizierungsgerät: Überprüfen, ob das Lesegerätkabel ordnungsgemäß an den Mini-DIN-Anschluss der Steuereinheit angeschlossen ist. Wenn das Kabel ordnungsgemäß angeschlossen ist und immer noch kein Licht aufleuchtet, mit dem nächsten Schritt fortfahren. **USB-Kartenlesegerät**: Sicherstellen, dass auf dem MFG die richtige Softwareversion läuft. Prüfen, ob das Kartenlesegerät richtig an das MFG angeschlossen ist. Leuchtet die LED auch bei richtigem Anschluss des Geräts nicht, das MFG aus- und wieder einschalten. Leuchtet die LED weiterhin nicht, ein Ersatzlesegerät anschließen.
2	Stromversorgung unterbrochen	**Authentifizierungsgerät:** Die Rückseite (Anschlussseite) der Steuereinheit prüfen. Wenn eine Stromversorgung vorhanden ist, leuchtet die gelbe Anzeige neben dem mit „Ethernet" bezeichneten Anschluss auf. Sicherstellen, dass das Netzkabel fest mit dem Gerät sowie mit dem Netzteil und der Wandsteckdose verbunden ist. Sicherstellen, dass die Wandsteckdose mit Strom versorgt wird.
3	LED auf dem Lesegerät blinkt langsam rot	**Authentifizierungsgerät**: Ein langsames Blinken der Lesegerätanzeige zeigt an, dass das Lesegerät korrekt an die Steuereinheit angeschlossen ist, aber dass die Steuereinheit keine Verbindung zum Server herstellen konnte. Sicherstellen, dass das Ethernet-Kabel an den mit „Ethernet" beschrifteten Anschluss und an die Ethernet-Wandsteckdose angeschlossen ist. **USB-Kartenlesegerät**: Das Lesegerätmodul des MFGs kann nicht mit dem Server kommunizieren. Sicherstellen, dass das MFG richtig an das Netzwerk angeschlossen ist und das Gerät richtig über Secure Access Manager initialisiert wurde.
4	Ethernet-LED aus	**Authentifizierungsgerät:** Wenn die grüne Anzeige neben dem mit „Ethernet" bezeichneten Anschluss nicht leuchtet, besteht keine Ethernet-Verbindung. Die Funktionstüchtigkeit des Ethernet-Patch-Kabels durch Tests mit einem anderen Kabel überprüfen und die Aktivität der Ethernet-Wandsteckdose verifizieren.

	Symptom	Anweisungen
5	Ethernet-LED leuchtet durchgehend grün	**Authentifizierungsgerät:** Wenn die grüne Anzeige neben dem mit „Ethernet" bezeichneten Anschluss durchgehend grün leuchtet, besteht zwar eine Ethernet-Verbindung, jedoch keine Aktivität. Überprüfen, ob die Ethernet-Wandsteckdose an den richtigen Hub oder Switch angeschlossen ist.
6	Gerät nicht in der Geräteliste des Secure Access-Servers aufgelistet	**Authentifizierungsgerät**: An der Secure Access-Konsole die Dropdown-Liste mit den Authentifizierungsgeräten aufrufen und prüfen, ob die MAC-Adresse des Problemgeräts aufgelistet ist. Wenn die MAC-Adresse des Geräts (siehe Etikett mit der Seriennummer auf der Steuereinheit) nicht aufgeführt ist, konnte es keine Verbindung zum Server aufnehmen. **USB-Kartenlesegerät**: USB-Kartenlesegeräte werden grundsätzlich nicht in der Geräteliste aufgeführt.
7	Gerät besitzt keine IP-Adresse	**Authentifizierungsgerät**: Wenn zur Konfiguration der Geräte DHCP genutzt wird, den DHCP-Server überprüfen, um sicherzustellen, dass dem Gerät eine IP-Adresse zugewiesen wurde (zur Prüfung die MAC-Adresse verwenden). Wenn keine IP-Adresse zugeordnet wurde, kann das Gerät entweder nicht mit dem DHCP-Server kommunizieren, oder die IP-Adresse wurde manuell konfiguriert.
8	Über DHCP vergebene Serveradresse nicht richtig	**Authentifizierungsgerät:** Bei Verwendung von DHCP für die Konfiguration der Geräte sicherstellen, dass der DHCP-Server den Wert 230 in der IP-Adresse des Servers verwendet. Sicherstellen, dass der Wert die korrekte IP-Adresse für den Server darstellt. Hinweis: Der Secure Access-Server selbst sollte nicht über DHCP konfiguriert werden. Wenn der Wert 230 nicht oder falsch festgelegt wurde, kann das Gerät den Server nicht kontaktieren.
9	IP-Adresse wurde manuell festgelegt	**Authentifizierungsgerät**: Wenn die IP-Adresse manuell eingerichtet wurde, die IP-Adresse des Geräts anhand der Aufzeichnungen ermitteln und über einen Webbrowser eine Verbindung zum Gerät herstellen. Wenn über die IP-Adresse des Geräts keine Webseite aufgerufen werden kann, ist das Gerät entweder nicht korrekt angeschlossen oder nicht kommunikationsfähig oder die IP-Adresse wurde falsch aufgezeichnet. Um die erste Möglichkeit auszuschließen, das Gerät mittels eines Crossover-Kabels direkt an den PC anschließen und einen erneuten Verbindungsversuch starten. Wenn die Verbindung steht, die Netzwerkeinstellungen und die Server-IP-Adresse auf Korrektheit prüfen.

	Symptom	Anweisungen
10	Gerät unter seiner IP-Adresse nicht erreichbar	**Authentifizierungsgerät**: Wenn das Gerät unter seiner IP-Adresse unter Verwendung eines normalen, am Downlink-Anschluss angeschlossenen Ethernet-Kabels nicht erreichbar ist, das Gerät auf die Standardeinstellungen zurücksetzen. Dazu die Steuereinheit von der Stromversorgung trennen, den Schlüssel einführen und in die Position „On“ drehen. Anschließend die Stromversorgung wiederherstellen. Nach 30 Sekunden den Strom ausschalten, den Schlüssel abziehen und den Strom wieder einschalten. Das Gerät müsste jetzt über die Standard-IP-Adresse 192.168.2.1 erreichbar sein. (Darauf achten, dass die Netzwerkeinstellung des PCs das Ansprechen dieser Adresse ermöglicht.) Wenn nun die Webseite des Geräts erreicht werden kann, entweder die Netzwerkinformationen manuell konfigurieren oder eine erneute DHCP-Konfiguration durch eine erneute Verbindung mit dem Netzwerk versuchen. Wenn die Webseite immer noch nicht erreicht werden kann, ist möglicherweise die Steuereinheit beschädigt.
11	LED auf Lesegerät blinkt bei Einführen einer Karte schnell rot	Ein schnelles, rotes Blinken der Lesegerätanzeige kennzeichnet einen ungültigen Karteneinleseversuch; der Secure Access-Server hat keinen gültigen Netzwerkbenutzer anhand der Kartendaten erkennen können. Das Lesegerät mit einer Karte eines Benutzers prüfen, die auf anderen Lesegeräten nachweislich erkannt wird. Wenn die Karten von keinem Lesegerät korrekt gelesen werden können, kann die Serverkonfiguration die Ursache sein. Zur Überprüfung der Serverkonfiguration an den Kundendienst wenden.
12	LED des Lesegeräts bleibt beim Durchziehen der Karte konstant rot	Bleibt die LED beim Durchziehen einer Karte rot, deutet dies darauf hin, dass die Karte nicht erkannt wird. Eine Magnetkarte ist eventuell mit einem anderen Standard verschlüsselt oder verkehrt herum oder in die falsche Richtung durchgezogen worden. Eine Transponderkarte oder eine Smartcard wurde eventuell nicht nah genug am Lesegerät vorgezeigt oder ist nicht kompatibel. Sicherstellen, dass die Einleseaktion korrekt durchgeführt wurde. Wenn die gleiche Karte auf anderen Lesegeräten desselben Standorts funktioniert, ist möglicherweise das Lesemodul defekt. Funktioniert die Karte auf anderen Lesegeräten nicht, den Kartenanbieter kontaktieren und die Kartentechnologie sowie die Kompatibilität mit Kartenlesegeräten anhand vorhandener Listen überprüfen.
13	LED des Lesegeräts wechselt beim Einlesen einer Karte auf Grün	Eine rote LED kennzeichnet eine aktive Secure Access-Sitzung. Das bedeutet, die Karte wurde korrekt gelesen und entspricht einem gültigen Secure Access-Benutzer. Wenn die LED auf Grün umschaltet, doch das MFG immer noch deaktiviert ist, ist das Secure Access-Gerät möglicherweise einem falschen MFG zugeordnet. Die Gerätekonfiguration in der Secure Access-Konsole prüfen, um festzustellen, ob das Secure Access-Gerät mit dem korrekten MFG verbunden wurde.

	Symptom	Anweisungen
14	MFG-Steuerpult immer entsperrt	Das Steuerpult des MFGs kann nur auf Geräten gesperrt werden, die Xerox Secure Access unterstützen. Überprüfen, ob das verwendete Modell unterstützt wird und die korrekte Firmware-Version darauf installiert ist.
15	Fehlermeldung „Failed to enable Follow-You printing“ und „Failed to enable Follow-You printing: no site specified“	Diese Meldungen können ausgegeben werden, wenn der Dienst „Release My Documents“ nicht richtig installiert wird. Siehe Fehlerbehebung beim Dienst „Release My Documents“ Seite 50.
16	Eingabeaufforderungen des Geräts (Titel/ Anmeldeaufforderung) werden nicht am MFG-Steuerpult angezeigt	Das Gerät in Secure Access Manager öffnen. Auf die Schaltfläche **Initialize Secure Access device** (Secure Access-Gerät initialisieren) klicken. Die Eingabeaufforderungen müssten nun angezeigt werden.
17	LED am Lesegerät nach MFG-Neustart rot	**USB-Kartenlesegerät**: Sicherstellen, dass auf dem MFG die richtige Softwareversion läuft.

Fehlerbehebung beim Dienst „Release My Documents“

Wird nach Installation dieses Diensts die Schaltfläche „Release my documents“ am MFG nicht angezeigt, muss die Installation möglicherweise unter Angabe spezifischer Parameter wiederholt werden. Kann das MFG aufgrund der vorliegenden DNS-Einstellung den Hostnamen des DCE-Servers nicht auflösen, können Geräte nicht richtig registriert werden. In diesem Fall die Installation mit den in der unten stehenden Tabelle aufgeführten Parametern wiederholen.

Die Exe-Datei des Diensts „Release My Documents“ befindet sich im Ordner „Tools“ auf dem Core Authentication Server. Zur Installation der erforderlichen Dateien ist die Administratorberechtigung auf dem CAS- und DCE-Rechner erforderlich.

1. Eingabeaufforderung öffnen und in den Ordner „Tools“ wechseln. Beispiel:
   c:\Programme\Xerox\SecureAccess\Tools\
2. Die Exe-Datei mit den in der unten stehenden Tabelle aufgeführten Parametern ausführen:
   saxeroxeipregistration.exe

   Hinweis: Die neue Installation unter Einsatz dieser Parameter kann direkt durchgeführt werden. Eine vorherige Deinstallation ist nicht erforderlich.

Parameter	Ergebnis
-i	IP-Adresse des MFGs, auf dem der Dienst installiert wird
-r	Registriert den angegebenen DCE-Server auf dem angegebenen MFG.
-d	Hebt die Registrierung des Diensts auf dem angegebenen MFG auf.
-v	Zeigt Daten zur Registrierung an. Mithilfe dieses Befehls kann die Installation des Diensts überprüft werden.
-u	Dient zur Angabe des Benutzernamens. Das entsprechende Konto muss eine Berechtigung zur Aktualisierung des Geräts besitzen.
-p	Dient zur Angabe des Kennworts. Das entsprechende Konto muss eine Berechtigung zur Aktualisierung des Geräts besitzen.
-c	Prüft die Geräteliste auf dem angegebenen CAS-Server und registriert den Dienst auf allen Xerox-MFG in dieser Liste.
/?	Ruft eine Liste aller Parameter für den Dienst auf.

Beispiel:

```
saxeroxeipregistration.exe -i 192.168.97.180 -r 192.168.97.137
```

IP-Adresse des MFGs **IP-Adresse des DCE-Servers**

Ergebnis: Der Dienst wird auf einem einzelnen MFG installiert und auf dem angegebenen DCE-Server registriert.

Aufrufen der Anzeige „Release My Documents“

Ist der Dienst „Release My Documents“ installiert (Anweisungen siehe Installationshandbuch), kann der Benutzer über die entsprechende Anzeige auf Warteschlangen mit geschützten Aufträgen zugreifen und eigene Aufträge nach Bedarf freigegeben oder löschen.

1. Nach der Authentifizierung die Betriebsartentaste drücken.
2. Schaltfläche **Zusatzdienste** antippen.
3. **Release My Documents** antippen.
4. Es werden nun sämtliche Aufträge des Benutzers, die im lokalen Druckserver angehalten wurden, angezeigt. Die nachfolgende Tabelle enthält Erläuterungen zu den verfügbaren Schaltflächen.

Schaltfläche	Funktion
Drucken	Einen oder mehrere Aufträge in der Liste auswählen und diese Schaltfläche antippen, um die Aufträge zu drucken und aus der Liste zu löschen. Ist eine Auflage über 1 eingestellt, muss diese mit **OK** bestätigt werden.
Drucken & speichern	Mithilfe dieser Schaltfläche werden die in der Liste ausgewählten Aufträge gedruckt und verbleiben in der Liste. Ist eine Auflage über 1 eingestellt, muss diese mit **OK** bestätigt werden.
Löschen	Einen oder mehrere Aufträge in der Liste auswählen und diese Schaltfläche antippen, um die Aufträge ohne Druckausgabe aus der Liste zu löschen.
Alle auswählen	Dient zur Auswahl sämtlicher Aufträge in der Liste.
Aktualisieren	Stehen auf dem DCE-Server neue Aufträge an, werden sie mithilfe dieser Schaltfläche in die Liste aufgenommen.
Details	Über diese Schaltfläche werden der Name des ausgewählten Auftrags, Datum und Uhrzeit der Übermittlung, der Name des ursprünglichen Zieldruckers und der Name des Clientcomputers, von dem aus der Auftrag gesendet wurde, angezeigt.
Ende	Ruft wieder die Anzeige „Zusatzdienste“ auf.

Einstellung der Auflage von Druckaufträgen

Nach der Authentifizierung kann die Druckauflage am Ziffernblock des MFGs eingegeben werden. Ist eine Auflage über 1 eingestellt, muss diese bei Auswahl von **Drucken** bzw. **Drucken & speichern** bestätigt werden. Ist die mit der Bestätigungsaufforderung angezeigte Auflage richtig, **OK** antippen, andernfalls **Abbrechen** antippen und über den Ziffernblock die richtige Auflage eingeben. Anschließend erneut **Drucken** bzw. **Drucken & speichern** antippen.

Wurde für den Druckauftrag ursprünglich eine Auflage von zwei Exemplaren eingestellt und werden bei der Auflageneinstellung am Gerät ebenfalls zwei Exemplare angefordert, so werden vier Exemplare des Dokuments ausgegeben.

Beenden einer Sitzung

In der Anzeige „Release My Documents“ **Ende** antippen, um zur Anzeige „Zusatzdienste“ zurückzukehren. Anschließend **Schließen** antippen, zum Abschluss der aktiven Sitzung die Taste **Alles löschen** zweimal drücken und in der nun angezeigten Bestätigungsaufforderung **Abmelden** antippen.